UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

APLICACION DE LA PLATAFORMA DE COMUNICACIONES UNIFICADAS AVAYA AURA EN UNA RED CORPORATIVA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

MIKHAIL KIN YUN CAM ORÉ

PROMOCIÓN
2006 - II

LIMA – PERÚ
2012

A mis padres Jorge y Liky,
a mis tíos Enrique y Enervina, y mi familia
por todo su apoyo para lograr esta meta

APLICACION DE LA PLATAFORMA DE COMUNICACIONES UNIFICADAS AVAYA AURA EN UNA RED CORPORATIVA

SUMARIO

El presente informe explica la aplicación de los servicios de una plataforma de comunicaciones unificadas en una red corporativa con la finalidad de brindarle movilidad y flexibilidad en la forma de comunicarse a los empleados.

Se resalta el desempeño de las comunicaciones de una empresa como una de las partes esenciales dentro de sus procesos, pudiendo este campo afianzar una mayor integración y colaboración entre los empleados, así como con los clientes y proveedores. Esta importancia ha sido bien entendida por los mayores fabricantes de soluciones de telecomunicaciones en el mundo, quienes han coincidido en que la unificación de servicios asegura el incremento de productividad y tiempo de respuesta de las empresas que implementen dichas soluciones.

Se detalla entonces las facilidades que brinda la plataforma Avaya Aura 6.1 y lo que se obtiene con el uso de cada una de ellas; se detallan los componentes que conforman esta plataforma, la funcionalidad de cada uno y la forma como encaja cada uno dentro de la red donde se van a aplicar. Dicha plataforma está basada en protocolo SIP aprovechando su flexibilidad para agregar determinadas características para el manejo de las sesiones.

Luego de puesta en servicio esta plataforma en un escenario real, se realizaron las verificaciones de los servicios y aplicaciones para el uso cotidiano de los usuarios finales, a quienes se les capacitó para un óptimo aprovechamiento de la plataforma.

Finalmente se detalla una estimación del costo total de todo el proyecto asociado a compra de servidores, teléfonos, gateway, etc.

ÍNDICE

INTRODUCCION

Este Proyecto de Ingeniería fue desarrollado con la finalidad de describir la aplicación de la plataforma Avaya Aura 6.1 en una red corporativa real de un Grupo empresarial, mostrando lo último en tecnología de Comunicaciones Unificadas del que puede ser el fabricante más importante del mundo de este tipo de soluciones. La plataforma descrita en este informe es la única en su tipo puesta en servicio en América del Sur a la fecha

Este informe está enfocado a la estructura de la red de telefonía del Grupo empresarial, tomando como escenario principal la red local de una de las empresas que conforman este Grupo, y es desde ahí que se administrarán los servicios para los usuarios locales y remotos demás empresas en la red corporativa.

El informe está divido en 6 capítulos:

- Capítulo I: En este capítulo se realiza el planteamiento de ingeniería del problema, para ello primero se describe el problema y luego se expone el objetivo del trabajo. Finalmente se hace una breve descripción del escenario sobre el cual se está trabajando y las limitaciones se deben tomar en cuenta.
- Capítulo II: En este capítulo se describe los protocolos SIP y MPLS, los cuales son utilizados para el manejo de las sesiones en la telefonía y el transporte de los datos a través de la WAN en la red corporativa del Grupo. Estos conceptos son necesarios para entender los términos y técnicas aplicables en el informe.
- Capítulo III: En este capítulo se describe todo lo concerniente a la plataforma Avaya Aura 6.1, la descripción de las entidades que conforman su estructura.
- Capítulo IV: En este capítulo se resume la puesta en servicio de cada componente y luego se describen las pruebas realizadas para la verificación de los servicios.
- Capítulo V: En este capítulo se hace una estimación de la inversión realizada por el lado del Grupo para la aplicación de la plataforma de comunicaciones unificadas.
- Capítulo VI: En este capítulo se hace una estimación de la inversión realizada por el lado del Grupo para la aplicación de la plataforma de comunicaciones unificadas.

CAPITULO I
PLANTEAMIENTO DE INGENIERIA DEL PROBLEMA

1.1. Descripción del Problema

Las telecomunicaciones se han convertido en una parte esencial de los procesos desarrollados dentro de cualquier empresa, sea cual sea el rubro en que se desempeñe pues promueven la obtención rápida de información y promueven la integración de todo su personal. Por lo tanto, se hace necesario entonces hacer posible el mantener comunicados a los empleados de las empresas de la mejor forma necesaria de acuerdo a las funciones que cumplan dentro de ellas. Un personal que trabaja en Fuerza de Ventas, y que la mayor parte del tiempo la pasa visitando clientes, tiene distintos requerimientos en los servicios de telecomunicaciones que los requerimientos de un gerente que tal vez viaja frecuentemente, o los requerimientos de una secretaria que requiere facilidades para realizar o atender llamadas de una manera simple, o quizás un jefe de planta que requiere tener sesiones de video para ver los materiales ubicados en otras sedes, o tal vez la empresa requiera salas de reuniones con capacidad de entablar videoconferencias y audio conferencias.

Ante esto surge la necesidad de implementar una plataforma de comunicaciones que haga una convergencia de estos y otros casos, independientemente del medio utilizado y que pueda mantener la estructura que se posea actualmente y que permita un equilibrado costo/beneficio entre la innovación tecnológica y el darle más facilidades al personal de las empresas para desempeñar sus funciones.

1.2. Objetivo

Describir la aplicación de la plataforma de Comunicaciones Unificadas Avaya Aura, que está diseñada para integrar aplicaciones en tiempo real de audio, video, presencia y mensajería con los recursos existentes de servicio de e-mail y equipos móviles para la Red Corporativa de un grupo empresarial, mejorando con dicha plataforma la productividad y capacidad de respuesta de sus empleados manteniendo siempre un equilibrio con los costos asociados, y dándoles mayor libertad de movilidad al poder acceder a los servicios sin importar el lugar y el momento en que se encuentren ni el equipo que estén utilizando.

1.3. Descripción del Escenario

El escenario considerado para este informe es un grupo empresarial que cuente con una red de datos ya desplegada (MPLS, ATM, Frame Relay, etc.) mediante la cual todas las empresas que conformen el grupo interconecten sus aplicaciones y comunicaciones, entre ellas las comunicaciones de voz. Si consideramos un grupo empresarial importante es factible que algunas de sus empresas tengan presencia en el extranjero y la red debe asegurar una integración óptima con todas las sedes de grupo.

Para el caso de comunicaciones de voz se considera a la central telefónica de cada sede como un nodo de la red corporativa, cada uno de estos nodos debe conectarse hacia la red con algún protocolo de VoIP, de preferencia para este escenario se considera el uso del protocolo SIP.

La plataforma de comunicaciones de este grupo está basada en una red de datos MPLS sobre la cual se comunican todas las centrales telefónicas existentes, las cuales son del fabricante Nortel (CS1000M, CS1000E, BCM50, BCM 400, BCM450) y se comunican entre sí con troncales SIP, cada central se comporta como una entidad SIP y en una de estas se utiliza la aplicación NRS de Nortel para el enrutamiento de todas las llamadas realizadas dentro de la Red Corporativa, junto con otro NRS secundario. Se cuenta también con un Plan de Marcado Numérico ya definido, la cual permite a los empleados de las empresas comunicarse unos a otros de manera interna y transparente, teniendo inclusive locales en el extranjero para el caso de algunas empresas del grupo.

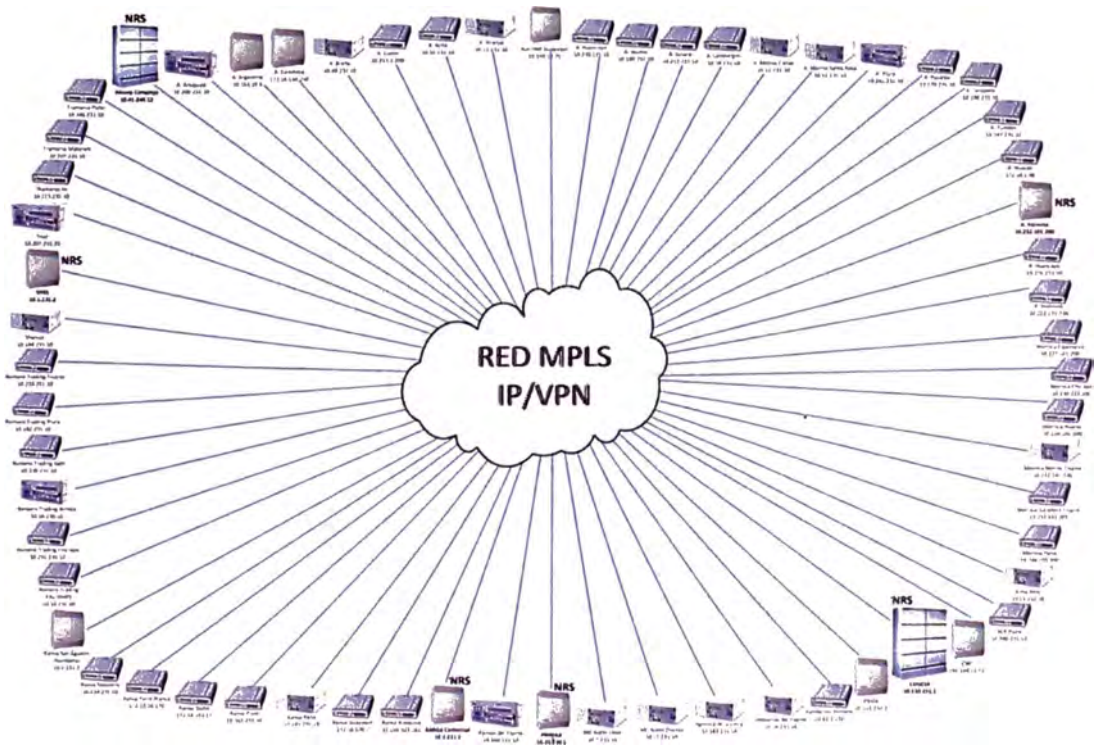


Fig 1.1 Escenario de Red Corporativa

1.4. Limitaciones del Problema

Entre las limitantes del problema podemos mencionar que para poner en servicio una plataforma como la que se desea se tiene que coordinar muchas veces con el personal que tiene a su cargo la administración de la red de datos del Grupo, personal de sistemas para solicitar la designación de un espacio físico donde instalar los servidores que conforman la plataforma en el Data Center respectivo, coordinaciones con los proveedores de racks y proveedores eléctricos para asegurar una correcta alimentación y un correcto aterramiento de dichos servidores, también hay que tomar en cuenta los tiempos que demora la entrega del hardware requerido (servidores, terminales telefónicos, etc.). Todo lo mencionado, sólo por mencionar algunos casos, influyó en los tiempos de avance de las distintas etapas que conforman la puesta en servicio de la plataforma.

Cabe señalar que para asegurar la correcta gestión de esta plataforma el administrador deberá contar con conocimientos de telefonía análoga, digital y sobre VoIP, conocimientos de protocolo SIP y MPLS, configuración de centrales Nortel (CS1000M, CS1000E, BCM50, BCM 400, BCM450) y Avaya, así como conceptos básicos de networking, redes celulares y configuración de equipos celulares. Todo esto a fin de garantizar la sostenibilidad de la red.

CAPITULO II
MARCO TEORICO

2.1. Protocolo SIP

"Session Initiation Protocol" o SIP (Protocolo de Iniciación de Sesión), es un protocolo de señalización definido por el "Internet Engineering Task Force" o IETF que permite el establecimiento, la liberación y la modificación de sesiones multimedia (RFC3261). Este protocolo hereda de ciertas funcionalidades de los protocolos "Hyper Text Transport Protocol" o "http", utilizados para navegar sobre el WEB y "Simple Mail Transport Protocol" o "SMTP", utilizados para transmitir mensajes electrónicos (e-mails). SIP se apoya sobre un modelo transaccional cliente / servidor como http. El direccionamiento utiliza el concepto "Uniform Resource Locator" o "URL SIP" parecido a una dirección E-mail. Cada participante en una red SIP es entonces alcanzable vía una dirección, por medio de una URL SIP. Por otra parte, los requerimientos SIP son satisfechos por respuestas identificadas por un código digital. De hecho, la mayor parte de los códigos de respuesta SIP han sido tomados del protocolo http. Por ejemplo, cuando el destinatario no esta ubicado, un código de respuesta «404 Not Found» esta devuelto. Un requerimiento SIP esta constituido de "headers" o encabezamientos, al igual que un mando SMTP. Se podría decir entonces que SIP, al igual que SMTP es un protocolo textual.

SIP ha sido extendido con el fin de soportar numerosos servicios tales como la presencia, la mensajeria instantánea (similar al servicio SMS en las redes móviles), la transferencia de llamada, la conferencia, los servicios complementarios de telefonía, etc. SIP ha sido elegido por el 3GPP para la arquitectura "IP Multimedia Subsystem" o "IMS" como protocolo para el control de sesión y el control de servicio. El remplazará en el futuro, los protocolos "ISUP", utilizado para el control de llamada en la Red Telefónica Conmutada, y "INAP", utilizado para el control de servicio en la arquitectura Red Inteligente.

El protocolo SIP es solo un protocolo de señalización. Una vez la sesión establecida, los participantes de la sesión intercambian directamente su trafico audio / video a través del protocolo "Real-Time Transport Protocol" o RTP. Por otra parte, SIP no es un

protocolo de reservación de recursos, y en consecuencia, no puede asegurar la calidad de servicio. Se trata de un protocolo de control de llamada y no de control del medio.

SIP tampoco es un protocolo de transferencia de fichero tal como "http", usado con el fin de transportar grandes volúmenes de datos. Ha sido concebido para transmitir mensajes de señalización cortos con el fin de establecer, mantener y liberar sesiones multimedia. Mensajes cortos, no relativos a una llamada pueden sin embargo ser transportados por SIP al estilo de SMS.

2.1.1. Entidades SIP

SIP define dos tipos de entidades: los clientes y los servidores. De manera más precisa, las entidades definidas por SIP son:

- El Servidor Proxy (Proxy Server): el recibe solicitudes de clientes que el mismo trata o encamina hacia otros servidores después de haber eventualmente, realizado ciertas modificaciones sobre estas solicitudes.
- El Servidor de Redireccionamiento (Redirect Server): se trata de un servidor quien acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones de red y las devuelve al cliente. De manera contraria al Proxy Server, el Redirect Server no encamina las solicitudes SIP. En el caso de la devolución de una llamada, el Proxy Server tiene la capacidad de traducir el numero del destinatario en el mensaje SIP recibido, en un número de reenvió de llamada y encaminar la llamada a este nuevo destino, y eso de manera transparente para el cliente de origen; para el mismo servicio, el Redirect Server devuelve el nuevo número (número de reenvió) al cliente de origen quien se encarga deestablecer una llamada hacia este nuevo destino.
- El Agente Usuario (User Agent) o "UA": se trata de una aplicación sobre un equipo de usuario que emite y recibe solicitudes SIP. Se materializa por un software instalado sobre un "User Equipment" o UE: una PC, un teléfono IP o una estación móvil UMTS.
- El Registrador (Registrar): se trata de un servidor quien acepta las solicitudes SIP REGISTER. SIP dispone de la función de registro de los usuarios. El usuario indica por un mensaje REGISTER emitido al Registrar, la dirección donde es localizable (dirección IP). El "Registrar" actualiza entonces una base de dato de localización. El registrador es una función asociada a un Proxy Server o a un Redirect Server. Un mismo usuario puede registrarse sobre distintas UAs SIP, en este caso, la llamada le será entregada sobre el conjunto de estas UAs.

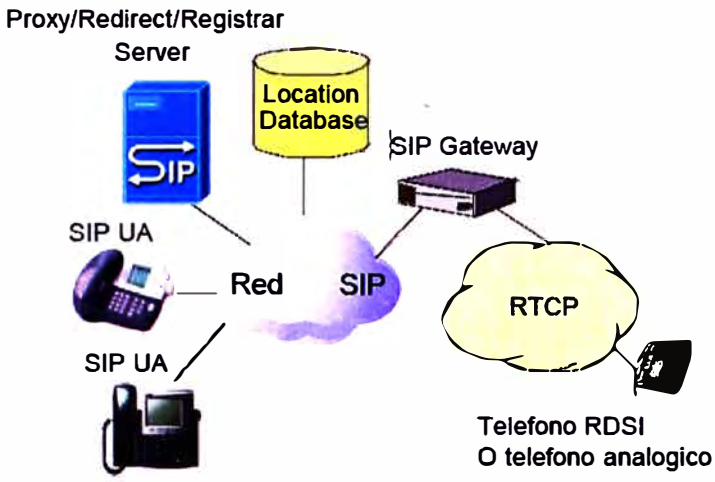


Figura 2.1 Entidades de una red SIP

2.1.2. Métodos y Respuestas SIP

A continuación se describen los métodos y respuestas SIP, que son los distintos mensajes que intercambian las Entidades SIP para el manejo de las sesiones.

a. Métodos SIP

El RFC 3261 define seis solicitudes / requerimientos o métodos SIP. El método **"INVITE"** es usado con el fin de establecer una sesión entre UAs. INVITE corresponde al mensaje ISUP IAM o al mensaje Q.931 SET UP y contiene las informaciones sobre el que genera la llamada y el destinatario así como sobre el tipo de flujos que serán intercambiados (voz, video, etc.).

Cuando un UA que emitió el método SIP INVITE recibe una respuesta final a la invitación (ejemplo : 200 OK), el confirma la recepción de esta respuesta por medio de un método **"ACK"**. Una respuesta del tipo "busy" o "answer" es considerada como final mientras una respuesta tipo "ringing" significando que el destinatario ha sido avisado es una respuesta provisoria.

El método **"BYE"** permite la liberación de una sesión anteriormente establecida. Corresponde al mensaje RELEASE de los protocolos ISUP y Q.931. Un mensaje BYE puede ser emitido por el que genera la llamada o el que la recibe.

El método **"REGISTER"** es usado por una UA con el fin de indicar al Registrar la correspondencia entre su Dirección SIP y su dirección de contacto (ejemplo: dirección IP).

El método **"CANCEL"** es utilizado para pedir el abandono de la llamada en curso pero no tiene ningún efecto sobre una llamada ya aceptada. De hecho, solo el método "BYE" puede terminar una llamada establecida.

El método **"OPTIONS"** es utilizado para interrogar las capacidades y el estado de un User Agent o de un servidor. La respuesta contiene sus capacidades (ejemplo: tipo de media siendo soportado, idioma soportado) o el hecho de que el UA sea indisponible.

b. Respuestas SIP

Después de haber recibido y interpretado un requerimiento SIP, el destinatario de este requerimiento devuelve una respuesta SIP. Existen seis clases de respuestas:

- Clase 1xx : Información, el requerimiento ha sido recibido y esta en curso de tratamiento
- Clase 2xx: Éxito, el requerimiento ha sido recibido, entendido y aceptado.
- Clase 3xx: Re-enrutamiento, la llamada requiere otros procesamientos antes de poder determinar si puede ser realizada.
- Clase 4xx: Error requerimiento cliente, el requerimiento no puede ser interpretado o servido por el servidor. El requerimiento tiene que ser modificado antes de ser reenviado.
- Clase 5xx: Error servidor, el servidor fracasa en el procesamiento de un requerimiento aparentemente valido.
- Clase 6xx: Fracaso global, el requerimiento no puede ser procesado por ningún servidor.

2.1.3. Funcionamiento del protocolo SIP

En esta parte del informe se describe el funcionamiento del protocolo SIP para el registro de Agentes así como el establecimiento y termino de sesiones.

a. Inscripción a la red SIP

El método "REGISTER" es utilizado por un "USER AGENT" con el fin de indicar a la función Registrar (físicamente implantada en un Proxy Server o un Redirect Server) la correspondencia entre su dirección SIP (ejemplo: sip:mcamo@avaya.com) y su dirección IP (ejemplo: sip:mcamo@192.190.132.20). La dirección IP puede ser estática u obtenida de modo dinámico por DHCP. La función Registrar actualiza entonces una base de datos de localización. Desde este momento, el User Agent puede recibir llamadas ya que se encuentra ubicado. Si un usuario SIP desea reenviar sus llamadas de su dominio corriente hacia otro dominio, (ejemplo: del dominio avaya.com al dominio nortel.com), solo tendrá que indicar a la función Registrar de avaya.com su dirección SIP en el dominio nortel.com. Cuando un mensaje INVITE debe ser entregado por el Proxy Server del dominio avaya.com a sip: mcamo@avaya.com, la base de datos actualizada por la función Registrar indica al Proxy Server que el mensaje tiene que ser relevado a sip:mcamo@nortel.com. Entonces, el Proxy Server efectúa una búsqueda por el DNS de

la dirección IP del Proxy Server del dominio nortel.com con el fin de relevar el mensaje SIP a encaminar al destino apropiado (sip:mcamo@nortel.com).

En una red IP Multimedia Subsystem o IMS, el Proxy Server corresponde a una entidad CSCF (Call State Control Function), mientras la base de datos de localización es representada por la entidad Home Subscriber Server o HSS. El HSS en el IMS por los móviles es un HLR conteniendo por otra parte el perfil del usuario para los servicios IMS suscritos.

b. Establecimiento y liberación de sesión SIP

En el ejemplo siguiente, el que llama tiene como URL SIP sip:mcamo@nortel.com, mientras la URL SIP del destinatario de la llamada es sip:jquinto@nortel.com (Figura 2.2)

Un mensaje de establecimiento de llamada SIP INVITE es emitido por parte del UA SIP del que llama al Proxy Server. Este ultimo interroga la base de datos de localización para identificar la localización del que es llamado (dirección IP) y encamina la llamada a su destino. El mensaje INVITE contiene distintos "headers" o encabezamientos obligatorios, entre los cuales la dirección SIP de la persona que llama "From", la dirección SIP de la persona que recibe la llamada "To", una identificación de la llamada "Call-ID", un numero de secuencia "Cseq", un número máximo de saltos "max-forwards". El encabezamiento "Via" es actualizado por todas las entidades que participaron en el enrutamiento del requerimiento INVITE. Eso asegura que la respuesta seguirá el mismo camino que el requerimiento.

Por otra parte, el requerimiento SIP INVITE contiene una sintaxis "Session Description Protocol" o SDP. Esta estructura consiste en varias líneas que describen las características del medio que "mcamo" necesita para la llamada.

"mcamo" indica que la descripción SDP utiliza la versión 0 del protocolo, que se trata de una sesión telefónica (m = audio), que la voz constituida en paquetes le debe ser entregada a la dirección de transporte (puerto UDP = 45450, dirección IP =192.23.34.45) con el protocolo RTP y utilizando un formato de codificación definido en el RFC "Audio Video Profile" o AVP y pudiendo ser G. 711 μ-law o G.728.

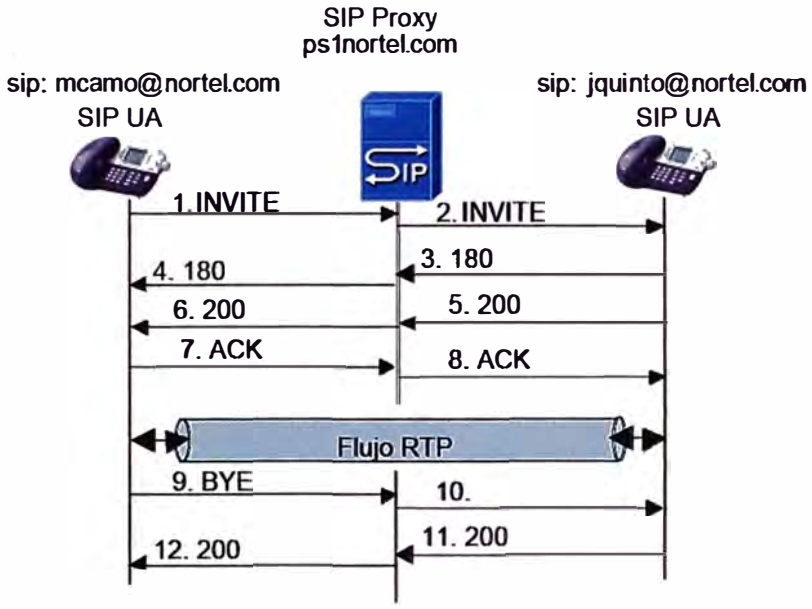


Figura 2.2 Establecimiento y liberación de sesión SIP

```
INVITE sip:jquinto@nortel.com SIP/2.0
Via : SIP/2.0/UDP station1.nortel.com:5060

Max-Forwards : 20
To : Jose Quinto <sip:jquinto@nortel.com>
From : Mikhail Cam <sip:mcamo@nortel.com>
Call-Id: 23456789@station1.nortel.com
CSeq: 1 INVITE
Contact: mcamo@192.190.132.20
Content-Type: application/sdp
Content-Length:162

v = 0
c = IN IP4 192.190.132.20
m = audio 45450 RTP/AVP 0 15
```

El destinatario devuelve luego una respuesta 180 RINGING al UA del que genera la llamada. Cuando el destinatario acepta la sesión, su UA emite una respuesta 200 OK encaminada hacia el UA del que genera la llamada.

```
SIP/2.0 200 OK
Via : SIP/2.0/UDP ps1.nortel.com:5060
Via : SIP/2.0/UDP station1.nortel.com:5060

Max-Forwards : 20
To : Jose Quinto <sip:jquinto@nortel.com>
From : Mikhail Cam <sip:mcamo@nortel.com>
Call-Id: 23456789@station1.nortel.com
CSeq: 1 INVITE
Contact: jquinto@192.190.132.27
Content-Type: application/sdp
Content-Length:162

v = 0
c = IN IP4 192.190.132.27
m = audio 22220 RTP/AVP 0
```

El UA del que genera la llamada devuelve un método ACK al destinatario, relevada por la entidad Proxy Server.

La entidad Proxy Server participa al encaminamiento de la señalización entre UAs mientras que las UAs establecen directamente canales RTP para el transporte de la voz o del video en forma de paquetes sin implicación del Proxy Server en este transporte.

Cuando "mcamo" cuelga, su UA envía un requerimiento BYE para terminar la sesión. Este requerimiento esta entregado al Proxy Server quien lo encamina a la UA de José. Este último, devuelve la respuesta 200 OK.

```
BYE sip:jquinto@nortel.com SIP/2.0
Via : SIP/2.0/UDP station1.nortel.com:5060

Max-Forwards : 20
To : Jose Quinto <sip:jquinto@nortel.com>
From : Mikhail Cam <sip:mcamo@nortel.com>
Call-Id: 23456789@station1.nortel.com
CSeq: 2 BYE
SIP/2.0 200 OK
Via : SIP/2.0/UDP ps1.nortel.com:5060
Via : SIP/2.0/UDP station1.nortel.com:5060
Max-Forwards : 20
To : Jose Quinto <sip:jquinto@nortel.com>
From : Mikhail Cam <sip:mcamo@nortel.com>
Call-Id: 23456789@station1.nortel.com
CSeq: 2 BYE
```

2.1.4. Extensiones del protocolo SIP

Una entidad SIP puede suscribir a un evento con el fin de ser notificada de su ocurrencia. El requerimiento **SUBSCRIBE** permite la suscripción mientras el requerimiento **NOTIFY** es utilizado con el fin de notificar (RFC 3265). El método **PUBLISH** permite publicar su estado.

El método **REFER** (RFC3515) reenvía el receptor hacia un recurso identificado en el método. REFER permite emular distintos servicios o aplicaciones incluyendo la transferencia de llamada. Contemplamos T1, la entidad que origino la transferencia, T2 la entidad transferida y T3, el destinatario de la transferencia. La transferencia de llamada permite a T1 transformar una llamada en curso entre T1 y T2 en una nueva llamada entre T2 y T3, elegida por T1. Si la transferencia de llamada se lleva a cabo, T2 y T3 podrán comunicar mientras que T1 no podrá seguir dialogando con T2 o T3.

El método **MESSAGE** (RFC 3428) ha sido propuesto como extensión al protocolo SIP con el fin de permitir la transferencia de mensajes instantáneos. La mensajería instantánea o "Instant Messaging" o "IM" consiste en el intercambio de mensajes entre usuarios en seudo tiempo real. Este nuevo método hereda de todas las funciones ofrecidas por el protocolo SIP tales que el enrutamiento y la seguridad. El requerimiento

MESSAGE puede transportar varios tipos de contenidos basándose sobre la codificación MIME.

El método **INFO** (RFC2976) permite transferir informaciones de señalización durante la llamada. Entre los ejemplos de información se encuentran los dígitos DTMF, las informaciones relativas a la tasación de una llamada, las imágenes etc...

Las respuestas finales 2xx, 3xx, 4xx, 5xx y 6xx a un requerimiento INVITE son satisfechas por el requerimiento ACK mientras las respuestas provisorias de tipo 1XX no son satisfechas. Ciertas respuestas temporarias tales como el 180 Ringing son críticas y su recepción es esencial para la determinación del estado de la llamada, entre otros durante el proceso de interconexión con la RTCP. El método **PRACK** (RFC3262) ha sido definido con el fin de satisfacer la recepción de respuestas temporarias de tipo 1XX.

El método **UPDATE** (RFC3311) permite a un terminal SIP actualizar los parámetros de una sesión multimedia (ejemplo: flujo media y sus codecs). El método UPDATE puede ser enviado antes de que la sesión sea establecida. UPDATE es entonces particularmente útil cuando se trata de poner al día los parámetros de sesión antes de su establecimiento, por ejemplo en puesta en espera del destinatario.

2.1.5. Interfuncionamiento entre SIP y RTC

Para el interfuncionamiento entre la Red Telefónica Conmutada RTC y SIP, es necesario introducir una pasarela o Gateway RTC/SIP que se interfase por una parte al RTC y por otra parte a una red SIP. Este Gateway cumple con dos funciones:

- Traducción de la señalización ISDN User Part o ISUP en señalización SIP y recíprocamente.
- Conversión de señales audio en paquetes RTP y recíprocamente; en efecto, este

Gateway establece canales lógicos RTP con la terminal SIP y establece circuitos de palabras con un switch o conmutador Class 4 o Class 5. El Class 5 Switch representa un conmutador telefónica de acceso mientras el Class 4 switch es un conmutador telefónico de transito. En el ejemplo contemplado en la figura 3, un terminal conectado a la RTC llama un UA SIP. El Class 5 Switch al cual esta conectado el que genera la llamada, emite un mensaje ISUP IAM al Gateway RTC/SIP. Este mensaje contiene el numero del destinatario, el identificador del circuito elegido por el Class 5 Switch para la llamada (Circuit Identification Code o CIC) así como informaciones indicando la naturaleza de la llamada (palabras, fax, datos, etc...).

El Gateway RTC/SIP traduce este mensaje en un requerimiento SIP INVITE que contiene una dirección de destino SIP de la cual el campo “user” es un número telefónico. Pasa el mensaje al SIP Proxy Server que obtiene la dirección IP del destinatario con la dirección SIP por medio de la interrogación de una base de datos o de un servidor de

localización. El mensaje INVITE esta relevado a la UA SIP. En paralelo, el Proxy Server notifica al Gateway la recepción del requerimiento INVITE por medio de la respuesta 100 Trying. El terminal SIP devuelve al Proxy Server una respuesta 180 Ringing para informar el que llama de la alerta del que esta llamado, mensaje relevado por el Proxy Server al Gateway. El Gateway traduce esta respuesta en un mensaje ISUP "Address Complete Message" o ISUP ACM enviado al Class 5 Switch. Este mensaje es traducido por el Class 5 Switch en un mensaje "Alerting" si el terminal que origina la llamada es una terminal RDSI o en una señal "Ringing Tone" en el caso de una terminal analógica.

Cuando el destinatario descuelga, una respuesta 200 OK esta devuelta al Proxy Server quien la releva al Gateway. El Gateway pone el recibí de esta respuesta por un requerimiento ACK encaminado por el Proxy Server al destinatario. En paralelo, el Gateway genera un mensaje ISUP Answer Message o ISUP ANM emitido al Class 5 Switch.

Este intercambio de señalización a permitido el establecimiento de canales RTP entre el terminal SIP y el Gateway así como la colocación de un circuito de voz entre el Gateway y el Class 5 Switch.

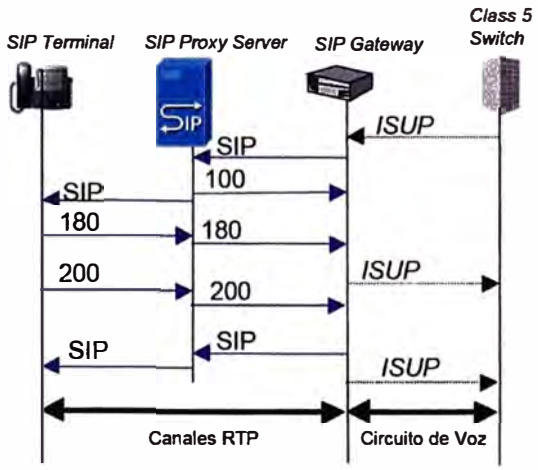


Figura 2.2 Interfuncionamiento RTC/SIP

Durante la fase de transferencia de información, el Gateway convierte las señales de audio recibidas sobre el circuito de voz en paquetes RTP enviados sobre los canales RTP y viceversa.

2.2. Protocolo MPLS

MPLS (Multi-Protocol Label Switching) es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios Prívate Line, Frame Relay o ATM.

Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Y todo ello en una única red. Contamos con distintas

soluciones, una completamente gestionada que incluye el suministro y la gestión de los equipos en sus instalaciones (CPE). O bien, que sea usted quien los gestione

MPLS (Multiprotocol Label Switching) intenta conseguir las ventajas de ATM, pero sin sus inconvenientes. Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la dirección de destino). MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS). La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS en la SLA. Por tanto MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente. El etiquetado en capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, Frame Relay, líneas dedicadas, LANs.

Las principales aplicaciones de MPLS son:

- Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente)
- Policy Routing
- Servicios de VPN
- Servicios que requieren QoS

2.2.1. Funcionamiento de MPLS

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP (Label Switching Path) por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSPs, uno en cada sentido.

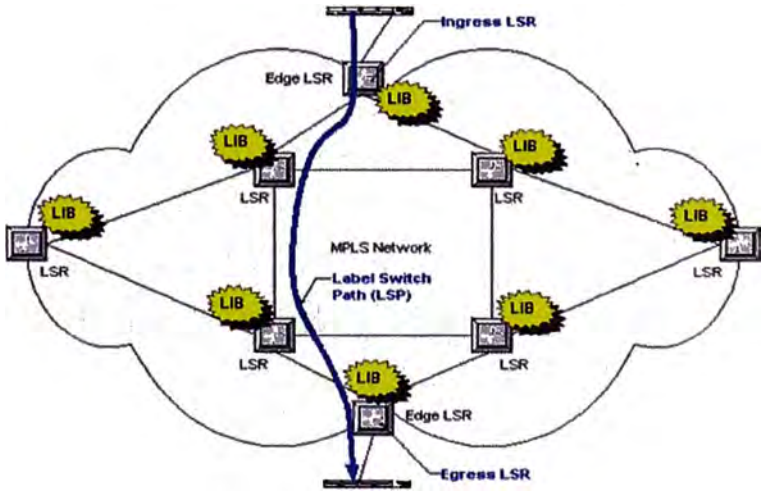


Figura 2.3 Ejemplo de LSP sobre una red MPLS

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR (Label Switching Router) que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío.

Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control, según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta. Tomando como ejemplo la Figura 2.4 vemos que a un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

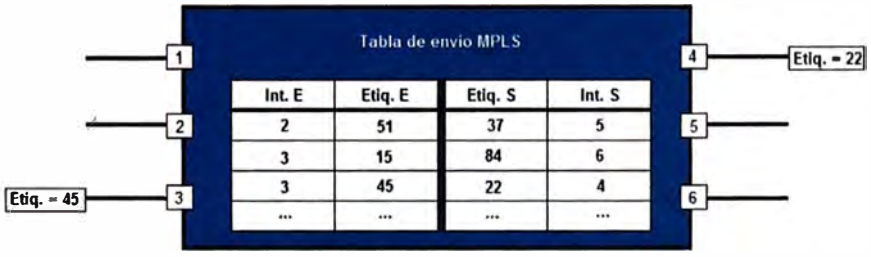


Figura 2.4 Ejemplo de Tabla de envío de un LSR

Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Swiching Router) a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

Cuando un paquete llega a un LSR, este le asigna una etiqueta y lo envía al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

La etiqueta MPLS se coloca delante del paquete de red y detrás de la cabecera de nivel de enlace. Las etiquetas pueden anidarse, formando una pila con funcionamiento

LIFO (Last In, First Out). Esto permite ir agregando (o segregando) flujos. El mecanismo es escalable. Cada nivel de la pila de etiquetas define un nivel de LSP , así dentro de una red MPLS se establece una jerarquía de LSP's. En ATM y Frame Relay la etiqueta MPLS ocupa el lugar del campo VPI/VCI o en el DLCI, para aprovechar el mecanismo de conmutación inherente.

Las etiquetas MPLS identifican a la FEC asociada a cada paquete. A continuación se muestra una etiqueta MPLS genérica:

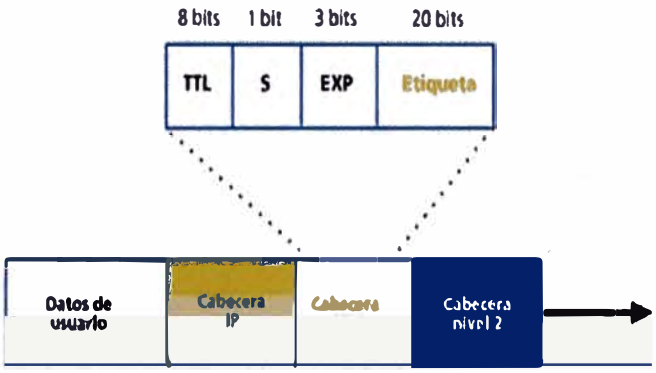


Figura 2.5 Ubicación de Cabecera MPLS

La cabecera MPLS se detalla de la siguiente forma:

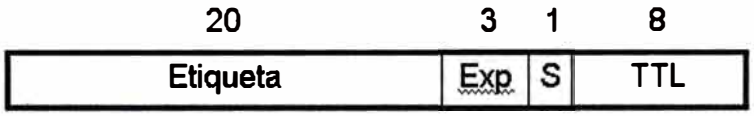


Figura 2.6 Detalle de Cabecera MPLS

Etiqueta: La etiqueta propiamente dicha que identifica una FEC (con significado local)

Exp: Bits para uso experimental, una propuesta es trasmitir en ellos información de DiffServ

S: Vale 1 para la primera entrada de la pila (la más antigua), 0 para el resto. Esta es la primera etiqueta introducida.

TTL: Contador del número de saltos. Este campo reemplaza al TTL de la cabecera IP durante el viaje del datagrama sobre a red MPLS.

A continuación se muestra la ubicación de la cabecera MPLS para diversos casos de capa 2:

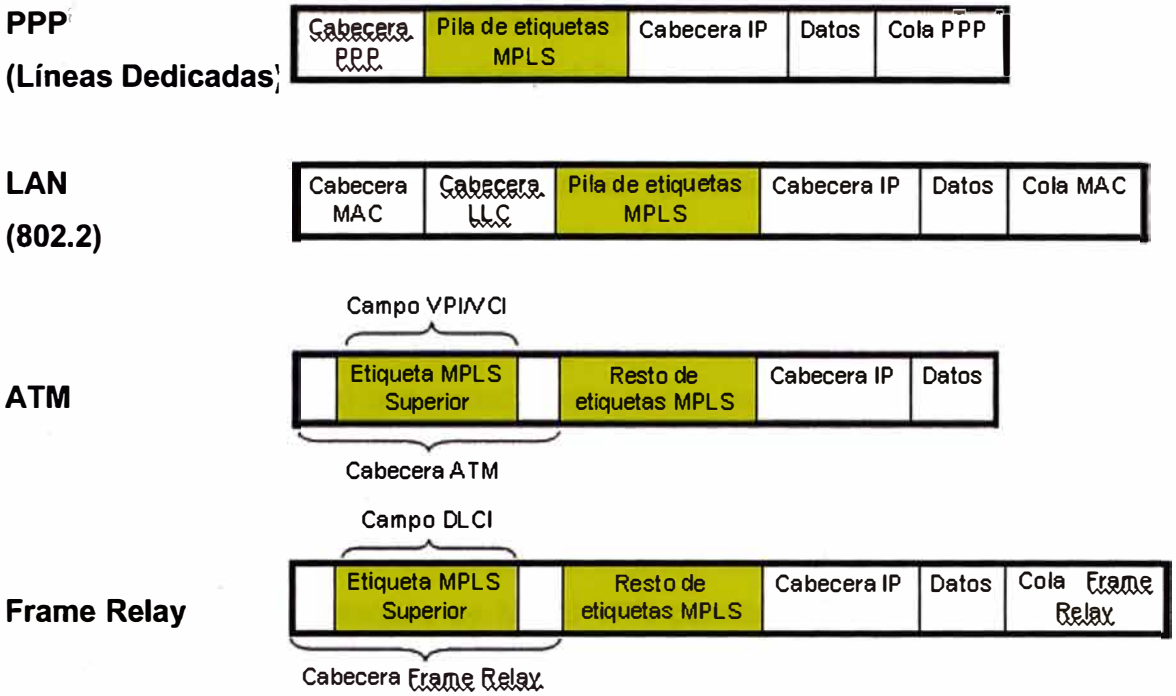


Figura 2.7 Cabecera MPLS en cada caso de capa 2

Los paquetes se envían en función de las etiquetas, no se examina la cabecera de red completa. El direccionamiento es más rápido. Cada paquete es clasificado en unas clases de tráfico denominadas FEC *(Forwarding Equivalence Class)*. Los LSPs por tanto definen las asociaciones FEC-etiqueta.

En los últimos tiempos, no sólo se viene hablando de la famosa convergencia de Voz, Video y Datos sobre una misma plataforma, sino también de la necesidad de la migración de servicios "Legacy" (heredados) como ATM o Frame Relay a una nueva generación de "IPbased VPNs" (Redes Privadas Virtuales basadas en protocolo IP) como los son las "MPLS VPNs" (Redes Privadas Virtuales basadas en Multiprotocol Label Switching).

A continuación, encontraremos 10 razones claves por las que una empresa, corporación u organismo puede pensar en migrar su infraestructura Legacy actual a una IP-Based MPLS VPN

- **Flexibilidad:** Cada empresa, corporación u organismo tiene desarrollada su propia estructura interna, tanto en infraestructura como en recursos humanos, generadas en base a sus necesidades y recursos disponibles. En base a ésta estructura, muchas veces única, se montan los servicios de comunicaciones para acomodar de la mejor manera posible y al menor costo, el transporte de la información interna, así como también externa, con sus clientes y proveedores.

  La topología de una MPLS VPN puede acomodarse acorde a cada necesidad, dada su naturaleza que brinda conexiones "Any-to-Any" (cualquiera con cualquiera)

entre los distintos puntos que comprenden la VPN, contando así con el mejor camino o ruta entre cada punto. A su vez se puede obtener mayor flexibilidad realizando configuraciones híbridas con Hub-and-Spoke (estrella), por ejemplo en las conexiones con clientes.

- **Escalabilidad:** Con un nuevo concepto de aprovisionamiento, llamado "Point-to-Cloud" (punto a la nube), se implementan los nuevos puntos de la VPN. Este concepto proviene del hecho de que cada vez que sea necesario "subir" un nuevo punto a la VPN, sólo habrá que configurar el equipamiento del Service Provider (Proveedor de Servicios) que conecte este nuevo punto. De esta forma, evitamos tareas complejas y riesgosas, como las que se producen cuando se activa un nuevo punto en una red basada en circuitos virtuales de Frame Relay o ATM, en donde es necesario re-configurar TODOS los puntos involucrados.
- **Accesibilidad:** La arquitectura de MPLS VPN permite utilizar prácticamente todos las tecnologías de acceso para interconectar las oficinas del cliente con su Service Provider. Por dicho motivo, la versatilidad que nos permite utilizar xDSL o un enlace Wireless Ethernet en las oficinas más pequeñas y hasta incluso en usuarios móviles, nos permite dimensionar cada punto de la VPN acorde a sus necesidades sin limitar o restringir la de otros puntos.
- **Eficiencia:** En una infraestructura 100% IP, es decir, aquellas empresas en donde todo el equipamiento involucrado y las aplicaciones utilizadas son basadas en IP, el uso de servicios de transporte ATM o Frame Relay someten al cliente a incurrir en un costo adicional por el overhead que los protocolos de transporte introducen. Mediante IFX MPLS VPN - un servicio IP-Based VPN - este costo extra desaparece.
- **Calidad de servicio (QoS) y Clases de servicio (CoS):** Las necesidades de comunicación entre dos lugares remotos, hoy en día van mucho más allá de la simple transferencia de datos vía email, web u otras aplicaciones. Siendo incluso insuficiente muchas veces, la interesante combinación de voz y datos bajo una misma plataforma. Es por ésto, que la ya mencionada Convergencia de datos con aplicaciones real-time y/o interactivas, voz y tambien video de alta calidad, necesitan de una eficiente plataforma de transporte.

  Mediante la utilizacion de técnicas y herramientas de Calidad de Servicio (QoS), se ofrecen distintas Clases de Servicio (CoS) dentro de una MPLS VPN para cumplimentar los requerimientos de cada servicio o aplicación.
- **Administración:** Las MPLS VPN son denominadas Network-Based, ésta característica proviene del hecho en que el servicio es implementado sobre la infraestructura del Service Provider; implicando, entre otras cosas, que la

administración de enrutamiento es llevada a cabo por el Service Provider; quien por su naturaleza, es especialista en dicha tarea desligando así al cliente de llevarla a cabo.

- **Monitoreo y SLAs:** Las MPLS VPN son monitoreadas, controladas y con un constante seguimiento en forma permanente, las 24 horas los 7 días de la semana, por parte del Service Provider. Además, se extienden "Service Level Agreements" (acuerdos de nivel de servicio) para garantizar y asegurar la estabilidad y performance que el cliente necesite.
- **Fácil Migración:** La simplicidad de la tecnología determina que las tareas de aprovisionamiento, administración y mantenimiento sean actividades sencillas para el Service Provider; lo cual se traslada directamente al cliente, obteniendo una migración del servicio actual sin complicaciones.
- **Seguridad:** Análisis y estudios realizados por los distintos fabricantes y entidades especializadas en el área, determinaron que los niveles de seguridad entregados por una MPLS VPN son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM.
- Sin embargo, en escenarios donde estos niveles no son suficientes, como por ejemplo en las necesidades de entidades financieras, una MPLS VPN puede también ser combinada con la encriptación y autenticación que IPSec brinda, elevando aún más la seguridad de la VPN.
- **Bajo Costo:** Son varios los motivos que permiten afirmar que un servicio MPLS VPN ofrece "más por menos", entre ellos podemos destacar: Independecia de equipos de cliente (CPE): al ser un servicio Network-based, la implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente.
- **Convergencia:** por ser una VPN CoS-Aware (Soporte de Clases de Servicio) se puede integrar distintos servicios y aplicaciones sobre una misma plataforma. De este modo, empresas que al día de hoy mantienen distintos y costosos servicios para soportar sus necesidades de voz, datos y video; pueden unificar estos requerimientos concluyendo en un ahorro significativo y manteniendo relación con un único proveedor de servicios.

2.3. Protocolo RTP

RTP (Real Time Protocol) es el protocolo que se encarga de transportar la voz propiamente dicha. Este protocolo trabaja sobre UDP y por lo tanto no hay mucho control de transmisión. Es decir que el equipo emisor envía la voz hacia al otro extremo con la esperanza de que llegue, pero no espera recibir confirmación de esto.

Si un paquete de voz se pierde en el camino simplemente se rellenará ese espacio con un silencio. Lo que técnicamente se llama ruido confortable (*comfort noise*). A pesar de encargarse de casi toda la labor de transportar la voz, RTP no está solo y tiene un protocolo de apoyo llamado RTCP. RTCP no es del todo indispensable pero proporciona valiosa ayuda al momento de transportar la voz de manera óptima pues proporciona estadísticas e información de control que le permiten a Asterisk o al otro extremo tomar decisiones para mejorar la transmisión en caso de ser posible. Por lo tanto, los paquetes RTCP se transmiten periódicamente para comunicar dicha información a los equipos de voz involucrados.

RTP permite:

- Identificar el tipo de información transportada.
- Añadir marcas temporales y números de secuencia de la información de transporte.
- Controlar la llegada de los paquetes.

2.3.1. Estructura de un paquete RTP

Un paquete RTP se compone de un encabezado y la data (o *payload*). En encabezado contiene alguna información interesante que explicaremos aquí, podemos ver en la Figura 2.8 cómo luce un encabezado RTP.

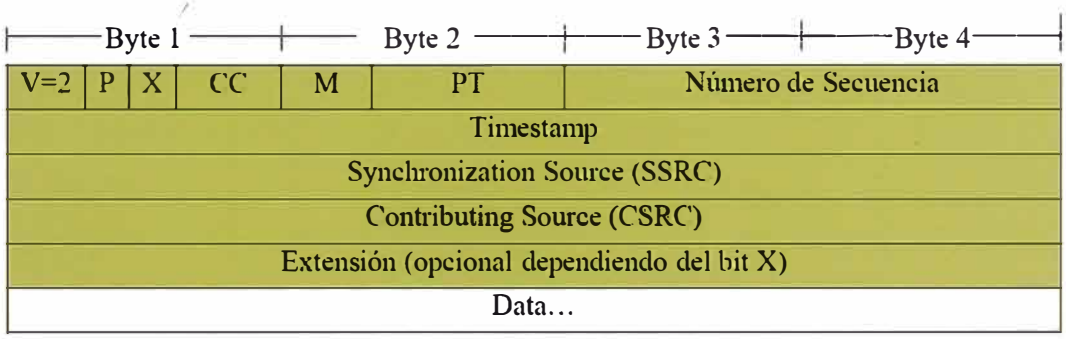


Figura 2.8. Cabecera RTP

A continuación se detalla cada campo de la cabecera RTP:

- **V:** es el número de versión. Este campo es de 2 bits de longitud y su valor contenido siempre es el número 2.
- **P:** (*padding)* es un bit que indica si hay relleno al final de la data o no. Si el bit está en uno quiere decir que si hay relleno. El relleno no es otra cosa que bytes adicionales al final del payload.
- **X:** o extensión es un bit que indica si hay extensión del encabezado
- **CC:** es un identificador de 4 bits que indica el conteo CSRC
- **M:** Marcador de un bit

- **PT:** Tipo de carga útil (*Payload Type*), es un identificador de 7 bits que nos indica el tipo de carga útil que contiene este paquete RTP. Ejemplos de tipos son G729, GSM, PCMU (G711 u-law), entre otros.
- **Número de Secuencia:** Es un número entero que identifica cada paquete del presente flujo de datos. Este es un identificador secuencial que se incrementa en uno con cada paquete transmitido. Ocupa 16 bits.
- **Timestamp:** representa el instante de tiempo en el que se comenzó a muestrear la data que está siendo transmitida en el payload. Ocupa 32 bits.
- **SSRC:** Identifica la fuente de sincronización ya que el mismo equipo puede estar "hablando" con diferentes fuentes de paquetes RTP. Es un número aleatorio de 32 bits por lo que hay la posibilidad (aunque la probabilidad es baja) de que este número se repita entre dos fuentes. Existen mecanismos para resolver este problema.
- **CSRC:** Es un número de 32 bits que identifica las fuentes contribuyentes para el payload

2.4. Protocolo RTCP

RTCP es un protocolo de control diseñado para funcionar junto con RTP. Se basa en la transmisión periódica de paquetes de control por parte de todos los participantes de la sesión.

En una sesión RTP, los participantes periódicamente envían paquetes RTCP para mantener la calidad de los datos y la información de los participantes de la sesión.

RFC 1889 define cinco tipos de paquetes que llevan información de control:

- **RR (Receiver Report):** Los Receiver Report son generados para los participantes que no son emisores activos. Especifica el número de paquetes recibidos, el número de paquetes perdidos, el jitter entre llegadas y el TimeStamp para calcular el retardo entre el emisor y el receptor.
- **SR (Sender Report):** Los SR son generados por emisores activos. Además de mantener la calidad de la recepción como en RR, contiene una sección de información del emisor, proporcionando información de sincronización, contadores de paquetes acumulados y número de paquetes enviados.
- **SDES (Source Description Items):** Contiene información para describir las fuentes.
- **BYE:** Indica el final de la participación.
- **APP (Application specific functions):** Funciones específicas de aplicación.

2.4.1. Estructura de un paquete RTCP

El encabezado RTCP lleva la siguiente información:

- **Versión** (2 bits);
- **Relleno** (1 bit): indica que existe relleno, cuyo tamaño se indica en el último byte;

- **Conteo de informes de recepción** (5 bits): cantidad de informes en el paquete;
- **Tipo de paquete** (8 bits): 200 para SR;
- **Longitud** (16 bits): longitud del paquete en palabras de 32 bits;
- (32 bits): identificación de la fuente remitente específica;
- **Marca de tiempo NTP** (64 bits);
- **Marca de tiempo RTP** (32 bits);
- **Conteo de paquetes del emisor** (32 bits);
- **Bytes del paquete del emisor** (32 bits): estadísticas;
- **SSRC-n** (32 bits): número de la fuente cuyo flujo se analiza.

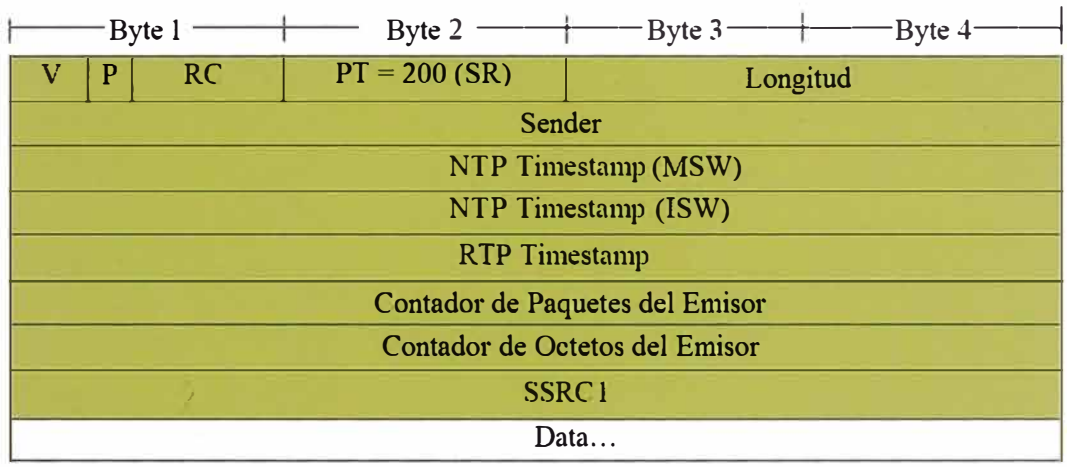


Figura 2.9. Cabecera RTCP

2.5. Redes Privadas Virtuales (VPN)

Una Red Privada Virtual (Virtual Private Network o VPN) es una forma de compartir y transmitir información entre un círculo cerrado de usuarios situados en diferentes ubicaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión; en nuestro caso de estudio las VPN se utilizan para que los empleados del Grupo puedan conectarse a su red estando fuera de ella utilizando Internet de por medio. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

De esta forma, una VPN consiste de un conjunto de sistemas o dispositivos interconectados a través de canales seguros, sobre una red pública, permitiendo el acceso remoto de los recursos y servicios de la red de forma transparente y segura como

si los usuarios estuvieran conectados de forma local. En nuestro caso los empleados del Grupo o utilizan para acceder a los servicios de Comunicaciones Unificadas vía remota.

Ofrece una alternativa sobre el acceso remoto tradicional y líneas dedicadas ya que utiliza los canales de comunicación ya existentes de la red de redes (Internet) permitiendo conectar usuarios remotos mediante el uso de servidores de VPN habilitando el uso compartido de los recursos ya que diferentes usuarios y conexiones pueden establecerse en diferentes momentos y compartir la misma infraestructura.

2.5.1. Tipos de Redes Privadas Virtuales (VPN)

VPN de acceso remoto: Este es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, etc.) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han remplazado con esta tecnología su infraestructura basada en módems y líneas telefónicas, aunque por razones de contingencia todavía conservan sus viejos módems.

VPN punto a punto: Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel RPV. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el punto anterior, también llamado tecnología de túnel o tunelado.

VPN interna WLAN: Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi). Un ejemplo clásico es un servidor con información sensible ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal autorizado pueda acceder a la información.

2.5.2. Características de las Redes Privadas Virtuales (VPN)

Una de las características principales de las VPN es la confidencialidad de los datos transmitidos, los cuales sólo pueden ser manejados y accesados por los usuarios

validados para ese fin, generando privacidad en la conexión sobre una red como Internet, la cual por sí sola no posee esa característica.

La comunicación entre sitios a través de Internet es vulnerable a ataques de "escuchas". El uso de una red privada virtual garantiza que todo el tráfico existente entre diferentes puntos de comunicación remotos interconectados mediante una red pública sea privado.

Una VPN permite crear un perímetro de seguridad de operación. Incorpora routers y corta fuegos como base, y por encima utiliza mecanismos de seguridad como son:

- Encriptación de datos: se utilizan varias técnicas (DES, 3DES, RSA)
- Compresión de datos
- Autenticación: el servidor RPV autentica al cliente para asegurarse que tienen los permisos necesarios. Si además el cliente autentica al servidor se protege contra la suplantación de servidores.
- Administración distribuida de claves
- Tunelado (Tunneling): para establecer las conexiones punto a punto.
- Acceso desde el exterior controlado por ser acceso remoto a un servidor seguro

Los protocolos empleados en estas redes son: PPTP (tunelado Punto-Punto), IPSec (Protocolo de Internet de Seguridad), L2TP (Protocolo de tunelado de Capa 2), GRE y SSH (Secure Shell) como recomendado si empleamos la administración distribuida de llaves.

También se utiliza el certificado digital para autenticar servidores, sitios remotos, empleados, socios y clientes, de forma que se garantice que sólo accedan a la organización usuarios autorizados y que cada uno sólo acceda a la información para la que tiene autorización.

2.5.3. Funcionamiento de las Redes Privadas Virtuales (VPN)

Es necesario instalar la VPN detrás del Corta fuegos corporativo y el router. El segundo paso es iniciar el intercambio de passwords y autenticación de servidores y sitios de forma que el administrador consiga un servidor seguro.

Los routers deben ser configurados para que envíen al servidor seguro la información a encriptar, dejando seguir su ruta normal al resto de tráfico. En el Corta fuegos se configura un puerto por el que pase la información al servidor seguro sin filtrarla.

Cuando la VPN recibe un paquete TCP/IP lo comprime y encapsula en un nuevo paquete especial para enviarlo por un túnel hasta su destino. El receptor desencapsula el paquete original, lo desencripta y lo envía a su destino dentro de la LAN.

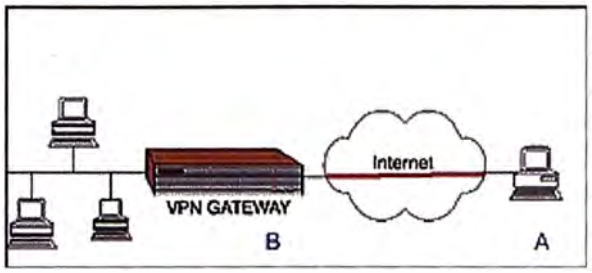


Figura 2.10 Red Privada Virtual

En la Figura podemos ver a un usuario A conectándose de manera remota a una red LAN utilizando una VPN tomando a Internet como medio de transporte. El VPN Gateway se encarga de autenticar al usuario y otorga los accesos respectivos a determinados recursos de la red. Este es el esquema sobre el cual los usuarios del Grupo accederán a los servicios de Comunicaciones Unificadas en nuestro caso.

2.5.4. Desventajas de las Redes Privadas Virtuales (VPN)

Entre algunas desventajas de utilizar VPN podemos mencionar:

- Las VPN pueden provocar una sobrecarga en la conexión de red debido a la encriptación utilizada.
- El tiempo de respuesta no está garantizado y, por lo tanto, no son recomendables para aplicaciones críticas.
- Si eventualmente, el ISP de algunos de los puntos pierde la conexión, la conectividad del enlace deja de existir entre esos puntos.
- Los anchos de banda reales son inferiores a los teóricamente contratados, pues no existe calidad de servicio.
- No todos los equipos actualmente instalados poseen facilidades para realizar RPVs. Además, se rigen por distintas normas y estándares y no son compatibles entre ellos.

2.6. Comunicaciones Unificadas

Las UC ofrecen todas las comunicaciones de una empresa y capacidades de colaboración juntas. Mejora la capacidad de administración y eficacia de una empresa y la hace más ágil. Las UC permiten a las empresas a desarrollar todo su potencial y, finalmente, obtener una ventaja sobre la competencia.

Las UC es la convergencia de todas las formas de audio, video, web, de escritorio y las comunicaciones móviles en una red IP que rompe todas las barreras de la distancia, el tiempo y los medios de comunicación, permitiendo a las personas comunicarse unos con otros en cualquier lugar, en cualquier momento, sobre cualquier dispositivo.

Se podría decir que las UC se basan en el concepto de dos elementos fundamentales y un número de otros relacionados, pero es opcionales. Los elementos fundamentales de la UC son:

Presencia: Es la capacidad de entender la disponibilidad y preferencias de comunicación de otro usuario. Las herramientas de Mensajería Instantánea (IM) han aumentado la conciencia de presencia de los usuarios, pero la tienen incorrectamente vinculados al chat. De hecho, la presencia puede asociarse no sólo a usuarios, sino también a dispositivos, como equipos médicos, sistemas de alarma y documentos de eventos, para acelerar flujos de trabajo y procesos de negocio.

VoIP: A largo plazo, los servicios de voz se integrarán en casi todas las aplicaciones de negocio. Debido a esto, VoIP es un componente crítico de la UC y una de sus tecnologías fundamentales. Los requisitos de fiabilidad, escalabilidad y seguridad ahora asociados con voz se extenderán a las aplicaciones y los medios necesarios para ofrecer todas las formas de la UC.

Existen componentes opcionales de la UC son los siguientes:

Buzón de voz: El correo de voz ha sido una característica estándar de telefonía desde hace años y es ampliamente utilizado a través de pequeñas y grandes empresas. La innovación en el espacio de las UC ha sido la de proporcionar un único buzón de voz al que se puede acceder desde múltiples dispositivos.

E-mail: Muchos componentes de la UC se integrarán en el e-mail, otra aplicación ampliamente desplegada.

Mensajería unificada: La convergencia de correo de voz y e-mail, esta es la forma más básica de la UC en tiempo no-real y ha sido alrededor de más de una década.

Cliente Móvil: La movilidad empresarial se está convirtiendo en un conductor clave para la UC. Un cliente móvil robusto permite a los usuarios el acceso sus herramientas de UC desde su dispositivo móvil.

Convergencia fijo-móvil (FMC): FMC permite a un trabajador mover sin problemas sus llamadas entre los teléfonos móviles y de escritorio, así como mantener el estado de una llamada entre celulares y redes LAN inalámbricas.

Conferencias multimedia integradas: Las aplicaciones de conferencia tienen más de una década, pero sólo recientemente han sido integradas por los proveedores de la UC. Esto incluye las conferencias de video, web y audio.

Chat / IM: La Mensajería instantánea se inició en el mundo social, pero rápidamente se convirtió en una herramienta corporativa. Es ampliamente utilizado en las empresas como una solución segura de comunicaciones corporativas.

Integración de Contact Center: Los Contact Center fueron unos de los primeros en adoptar la integración de telefonía en aplicaciones de negocio. Proporcionar pantallas "pops-up" y otras funciones de telefonía mejoradas ha permitido a los agentes de Contact Center agilizar y mejorar los procesos de servicio al cliente.

Estos son los principales componentes de la UC, pero otras aplicaciones de telefonía o presencia tales como el reconocimiento de voz y soluciones de teletrabajador como softphone o click-to-call podrían ser incluidas. El Cuadro 1 muestra la tasa de penetración de las aplicaciones de UC hasta el 2010.

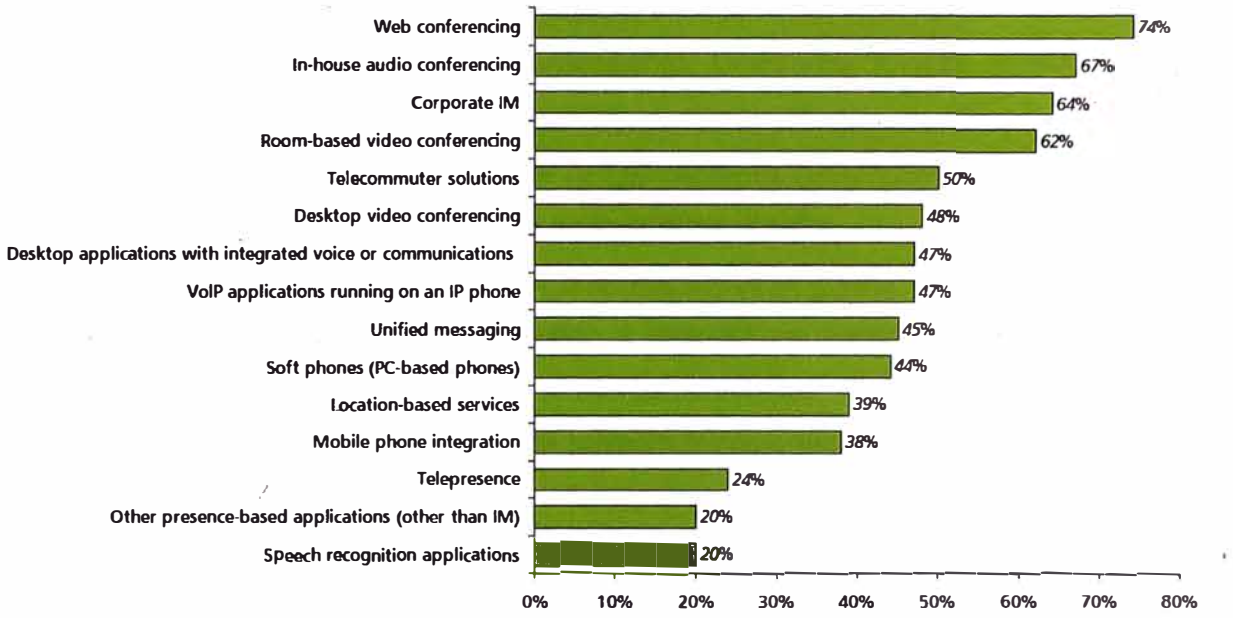


Figura 2.10. Aplicaciones UC más desarrollas (2010)

CAPITULO III
PLANTEAMIENTO DE LA SOLUCION APLICANDO AVAYA AURA

3.1. Comunicaciones Unificadas de Avaya

Se eligen la Plataforma de Comunicaciones Unificadas AVAYA AURA 6.1 por diversos motivos, entre los cuales resalta más:

- El poder integrar mundos diversos de comunicaciones como TDM, SIP y H.323, cosa que plataformas de otros fabricantes no lo pueden ofrecer.
- La presencia de Avaya en Perú con una filial en Lima y todo un equipo de soporte local y extranjero es un gran respaldo y asegura un soporte adecuado frente a contingencias o requerimientos que se puedan presentar.
- El posicionamiento en el mercado de telecomunicaciones que consigue de la fusión Avaya/Nortel (aproximadamente 30% del mercado mundial en telefonía)
- Poder satisfacer a los clientes del Grupo mediante la mejora de la disponibilidad y capacidad de respuesta de las empresas que lo conforman.
- Lograr hacer más rápidos los procesos de las empresas del Grupo.
- Reducción de Costos en las comunicaciones corporativas y aumento de productividad de sus empleados.
- Contar la primera plataforma de este producto desarrollada en el Perú y uno de los primeros en Latinoamérica, manteniendo al Grupo a la par con el avance en las telecomunicaciones.

3.2. Avaya Aura

Avaya Aura simplifica las arquitecturas existentes de comunicación mediante voz y video (que incluyen redes de múltiples vendedores), lo que da lugar a un concepto importante para las empresas: más capacidades con menor costo y complejidad.

Avaya Aura va más allá de la telefonía y de las redes de comunicación de datos existentes e introduce una plataforma que unifica todas las formas de comunicación (voz, mensajería, correo electrónico, correo de voz y más) haciendo uso de tecnologías establecidas y existentes como SIP, H.323, WiFi, GPRS e IMAP4, no siendo necesario introducir una tecnología nueva o crear un entorno exclusivo. Además de esto Avaya

Aura permite la interoperabilidad de con múltiples vendedores ofreciendo enruamiento SIP entre PBX nuevas y antiguas de Cisco, Nortel, Siemens y otros, lo que permite integrar sistemas TDM anteriores con gateways SIP. Al lograrse tal integración las empresas pueden implementar un Plan de Marcación único (en nuestro caso de estudio ya contamos con uno); así como un control de la manera en que las llamadas usan la red corporativa y comparten servicios externos, y del momento y lugar en que las llamadas "abandonan" la red y entran la red telefónica pública conmutada (PSTN) local.

Todo lo mencionado se potencia con la facilidad de presencia para indicar la disponibilidad y actividad de cada usuario. Estos servicios de presencia podrían colaborar con otras aplicaciones como el Communication Server de Microsoft Office, Lotus Sametime de IBM, etc.

Avaya Aura trabaja con una gama completa de clientes de la familia One-X de Avaya, como One-X Communicator y One-X Mobile; además de los productos de Flare Experience como Avaya Desktop Video Device (ADVD) y Flare Communicator. Adicionalmente se tiene la opción de soluciones para conferencias de video punto a punto.

3.3. Estructura de Avaya Aura

A continuación se describen los principales elementos de la plataforma Avaya Aura que se instalarán en la Red Corporativa y sus funciones.

3.3.1. Avaya Communication Manager

Es la parte central de las aplicaciones de Avaya. Es un software basado en Linux ejecutándose sobre una variedad de servidores S8XXX y proporciona control sobre los Avaya Media Gateways y terminales Avaya. Proporciona también la funcionalidad de sistema de gestión, ruteo de llamadas inteligente, integración de aplicaciones y manejo del networking para las comunicaciones empresariales. Permite un Plan de Numeración hasta de 7 cifras, tiene las configuraciones de los anexos, troncales, facilidades de restricciones de acceso, anuncios de voz, funciones de facilidad y coberturas de llamadas; así como configuración de perfiles de agentes, skills y vectores de call center, entre otras configuraciones.

3.3.2. Avaya Session Manager

La plataforma Avaya Aura se desarrolla sobre el software de Communication Manager que sabemos que es confiable, extensible y basado en IP, con el Avaya Session Manager se agrega una nueva capacidad en SIP, que al ser protocolo abierto hace posible unificar medios, modos, redes, dispositivos, aplicaciones y la presencia en tiempo real en una infraestructura común, lo que simplifica la administración de la plataforma. Avaya Session Manager tiene control sobre el software de Communication Manager y su

enrutamiento basado en SIP provee más capacidades de control centralizado y mejoras significativas en escala, posibilitando implementaciones más rentables y mucho más distribuidas. Se podrían tener hasta 10 Session Manager en una misma plataforma para temas de redundancia o balanceo de carga.

Avaya Session Manager hace posible el registro en integrar extensiones SIP a la plataforma Aura con servicios de localización, registro y proxy SIP. Esto permite el rastreo SIP y visualización de pistas.

Las llamadas desde y hacia usuarios en una PBX de terceros (por ejemplo las centrales Nortel de la Red Corporativa) se pueden direccionar hacia el Avaya Session Manager y utilizar las aplicaciones de la plataforma desde y hacia estos terminales. Toda entidad SIP (hasta 25000) puede conectarse directamente al núcleo de Avaya Session Manager siempre y cuando sea plenamente compatible con los estándares SIP.

Para las conexiones con la PSTN pueden realizarse con un Gateway (por ejemplo G450 o G860, por mencionar algunos) también por SIP.

3.3.3. Avaya System Manager

System Manager es un sistema de gestión central con interface web para instancias multiples de Avaya Session Manager, y ha sido diseñado para gestionar todos los componentes de la plataforma Aura. Permite una gestión centralizada de usuarios, políticas de enrutámiento, funciones de operaciones y monitoreo de fallas y de rendimiento.

Con respecto al rastreo SIP, y aprovechando que Avaya Session Manager maneja las sesiones SIP con una arquitectura central, el Avaya System Manager se puede establecer criterios de rastreo detallado y acciones de rastreo tan específicas como una única llamada, e tipo de llamada o el tráfico en general.

3.3.4. Avaya Presence Services

Los servicios de presencia es un elemento fundamental en UC, permitiendo a los usuarios conectar con la persona adecuada en el momento adecuado aprovechando los múltiples canales de las comunicaciones a su disposición. Avaya Presence Services proporciona información de presencia de telefonía y presenta un panorama de la disponibilidad del usuario y dispositivo publicando el estado en todos los medios posibles. Por medio de estos servicios de presencia os usuarios pueden intercambiar mensajería instantánea e información sobre presencia con los usuarios de Microsoft OCS (por ej., clientes de Microsoft Communicator).

3.3.5. Avaya One-X Client Enablement Services

Es un conjunto de aplicaciones que ofrece UC a algún handset de escritorio o al teléfono móvil, permitiendo acceso a capacidades UC como telefonía, mensajería,

movilidad y presencia, todo esto con aplicaciones de la familia One-X que actúan todas con un solo servidor. One-X Client Enablement Services soporta una interface web, un aplicativo ejecutable y una interface móvil (todos de la familia One-X) para accesar a las funcionalidades del servidor. Cabe mencionar que este servidor trabaja en sincronización con el Directorio Activo de la empresa donde quiera habilitar sus funciones.

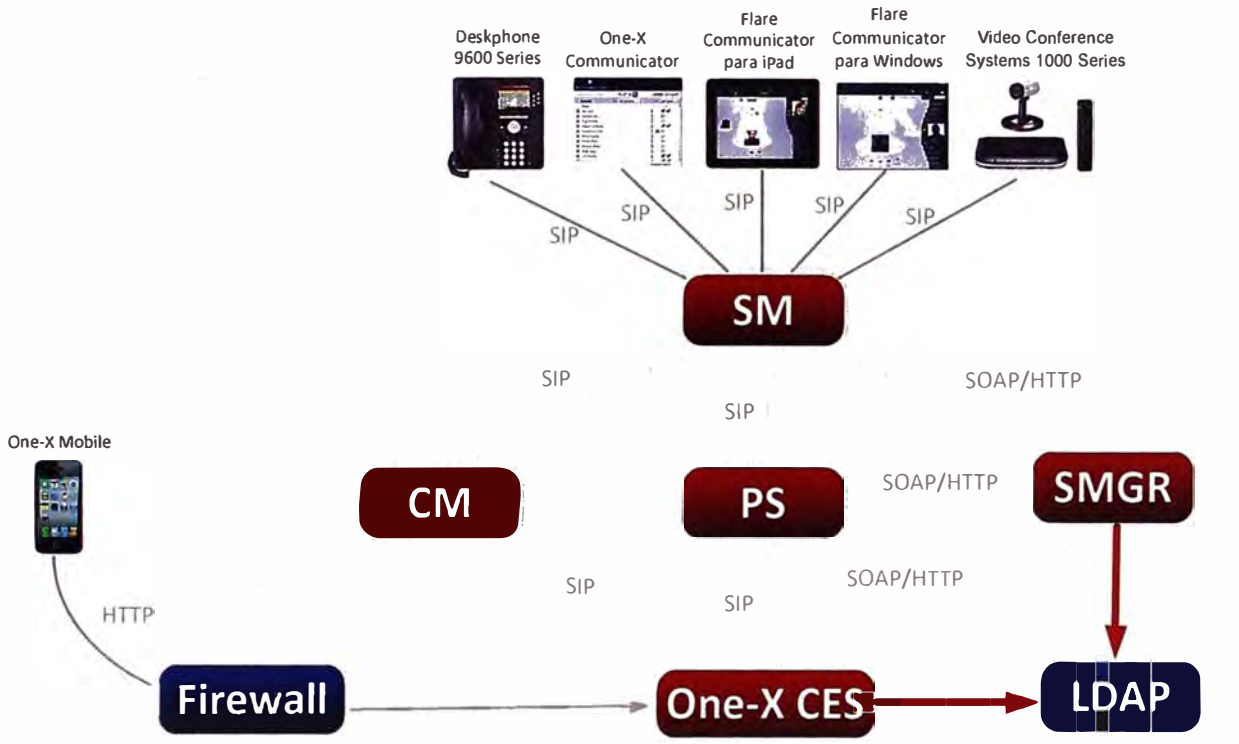


Figura 3.1 Diagrama Funcional de Avaya Aura 6.1

3.3.6. Gamma de productos Avaya One-X

La gama One-X de Avaya es una cartera de soluciones de UC que proporciona una experiencia sistemática y potente en las comunicaciones para el usuario final en diversos dispositivos e interfaces con el fin de impulsar la productividad y la ventaja competitiva. Las herramientas de colaboración que ofrece esta gama incluyen soluciones de movilidad, presencia, mensajería y conferencias de audio y video.

a. Avaya One-X Communicator

Avaya One-X Communicator es un cliente de UC que puede trabajar en SIP y H.323 y ofrece a los usuarios de las empresas un acceso sencillo e intuitivo a sus herramientas de comunicación diarias, aumentando su capacidad de respuesta y colaboración independientemente del lugar donde estén trabajando. Este cliente es una combinación de una aplicación de softphone con las funciones de presencia brindando las siguientes características:

- Correo de voz visual viendo el listado gráfico de mensajes y reproduciéndolos
- Conferencia de voz visual mostrando el listado de asistentes (por nombre o por teléfono) con opción de silencia a los asistentes o a uno mismo.
- Soporta conferencias ad hoc.
- Registro de llamadas salientes y entrantes independiente del teléfono que se haya usado (deskphone, softphone, equipo celular, etc.)
- Registro de mensajes instantáneos locales en la oficina.
- Permite manejar la presencia de forma automática o manual y personalizarla con algún mensaje personal.
- Soporta códecs G.711, G.723.1, G.729, G.729b y G.722
- Integración con Active Directory, IBM Lotus Notes, Microsoft Office Communicator, Microsoft Outlook, Microsoft Internet Explorer, Mozilla Firefox.

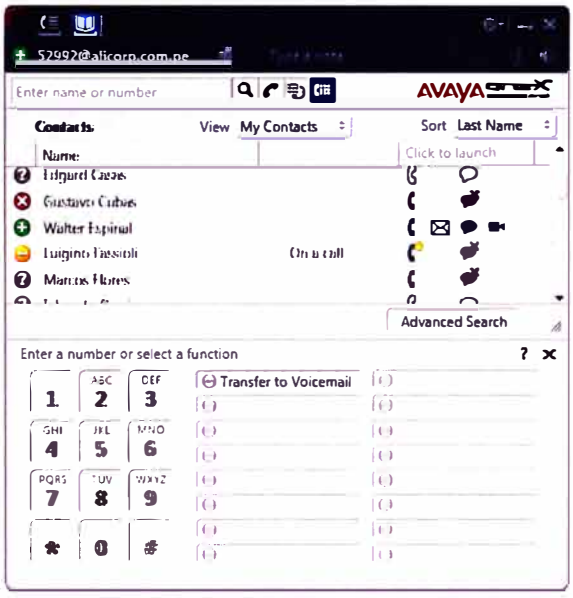


Figura 3.2 Interface de One-X Communicator

b. Avaya One-X Mobile

Las necesidades de los empleados son diferentes dependiendo del departamento donde trabajen y la función que desempeñen en la organización del Grupo. Ya sea con una integración directa con la plataforma de Avaya Communication Manager o con una integración de aplicaciones más amplia, Avaya One-X Mobile puede cumplir los requisitos de los empleados y del Grupo.

Este cliente se basa en una funcionalidad básica que las plataformas de Avaya ya disponen desde el 2001: Extensión al Celular. Esta funcionalidad permite crear del teléfono de escritorio al dispositivo móvil utilizando un único número de anexo. Esta solución basada en software es la base para la gama de clientes Avaya One-X Mobile y

se puede implementar fácilmente instalando un cliente en el dispositivo móvil y activando una licencia en la plataforma Avaya Aura. Estos clientes Avaya One-X Mobile amplían las funciones de la Extensión al Celular y permiten un acceso rápido a las funciones del teléfono de escritorio.

Entre algunas de las facilidades que se tienen en el Cliente One-X Mobile instalado podemos se pueden mencionar:

- Mantener un número único para llamadas entrantes. En caso el usuario cuente con un número directo, el tratamiento de la llamada será transparente para la persona que llama.
- Mantener un número único para llamadas salientes. Cuando el usuario efectúe una llamada desde su equipo móvil, la persona llamada verá el mismo número telefónico como en si la llamada haya sido hecha desde el teléfono de escritorio.
- Enrutamiento de llamadas. Las llamadas entrantes a la oficina pueden ser enrutadas a cualquier dispositivo mediante por programación o en forma ad hoc en la ubicación del anexo mediante una función.
- Listas VIP. Cualquier llamada que no esté en las listas VIP se enviará directamente al correo de voz para reducir el mínimo de interrupciones.
- Marcación de extensiones. Los usuarios pueden realizar llamadas mediante los planes de marcación de extensiones internas, tal y como harían en la oficina.
- Único buzón de Voz. Si una llamada no es respondida en el dispositivo móvil, esta es devuelta al sistema de correo de voz de la oficina, el mismo que utilizan los teléfonos de escritorio.
- Correo de Voz Visual. Los usuarios pueden ver el correo de voz de la oficina y de esta forma establecer la prioridad de los mensajes y ver los más importantes primero. Estos mensajes son guardados luego en formal local.
- Integración con Directorio Corporativo. Los usuarios tienen un fácil acceso a los contactos corporativos con una función de búsqueda.

En nuestro caso se aplicarán lo siguientes clientes de OneX Mobile:

- Avaya One-X Mobile para Android (versiones 2.2+)
- Avaya One-X Mobile para Blackberry (versiones RIM 5.0+)
- Avaya One-X Mobile para iPhone (versiones 3.0+)

Figura 3.3 Interfaz de One-X Mobile para iPhone

c. Avaya One-X Deskphone 9600 Series

Parte de la gamma Avaya One-X también incluye los teléfonos Serie 9600 que manejan una interfaz muy intuitiva que permite al usuario realizar las tareas básicas de telefonía como entablar una llamada de conferencia o realizar una transferencia.

Los equipos más recientes de esta gamma permiten el uso de PoE Clase 1, soportan un puerto Gigabit Ethernet y tienen pantalla táctil a colores, además manejan un ahorro de energía entre 40 y 60% cuando no están siendo utilizados. Estos teléfonos además pueden trabajar con señalización H.323 o SIP dependiendo de lo que requiera la plataforma.

Los equipos de la serie 9600 pueden adecuarse a gusto del usuario pues posee teclas softkeys en las que se pueden programas las funciones que se requieran como desvíos, marcados automáticos, parqueo de llamadas, o funciones especiales como el EC500.

Figura 3.4 Modelos de muestra Serie 9600

3.3.7. Avaya Video Collaboration Solutions

A continuación se describen las soluciones de colaboración de Avaya que se utilizan en el presente informe. Estas soluciones están orientadas a dar una calidad en alta definición consumiendo el menor ancho de banda posible para conferencias de video o de audio, en una variedad que va de acuerdo a la necesidad del usuario.

a. Avaya Desktop Video Device

Avaya Desktop Video Device es un dispositivo basado en Android que simplifica al usuario la forma de acceder e interactuar con sus herramientas de comunicación y colaboración dado que integra presencia, audio, web y videoconferencias a sus

aplicaciones empresariales, todo junto vía pantalla táctil de 11.6" y una interfaz amigable e intuitiva. Esta herramienta, que se comunica con la plataforma vía SIP, permite:

- Combina las comunicaciones por voz, video, correo electrónico, IM y redes sociales (Facebook y Twiter) con las aplicaciones corporativas, posibilitando la colaboración efectiva, eficiente y productiva.
- Los usuarios pueden acceder a los servicios Microsoft Exchange, como correo electrónico, contactos y agenda, directamente desde su tarjeta de contactos
- Permite filtrar historial de correos, mensajería instantánea y recordatorios relacionados con algún tema específico.
- Permite adaptar las herramientas de acuerdo a la preferencia del usuario.
- Brinda capacidades de videoconferencias punto a punto sin necesidad de algún servidor, integraciones de PC para el manejo de documentos y movilidad dentro o fuera de la empresa.
- Permite conexiones WiFi y bluetooth.

Figura 3.5 Avaya Desktop Video Device

b. Avaya Flare Communicator

Avaya Flare Communicator es un aplicativo SIP que cuenta con 2 versiones: una que está dirigido a los usuarios que utilicen los dispositivos iPad2 de Apple, ellos pueden descargar desde el App Store este aplicativo sin costo brindado por Avaya; y la otra que es la versión para Windows con un software fácil de instalar. Con estas dos alternativas los usuarios tendrán en sus tabletas y en sus computadoras la misma interface que se observó en el Avaya Desktop Video Device.

Este aplicativo les proporciona a los empleados y sus compañías funcionalidades como identificar desde la tarjeta de contacto si los empleados se encuentran disponibles y enviar un mensaje instantáneo, un correo electrónico o hacer una llamada de voz con sólo tocar la pantalla o haciendo un clic, dependiendo del dispositivo usado. Adicionalmente las videoconferencias punto a punto son posibles únicamente para la versión para Windows por el momento utilizando la cámara de la PC.

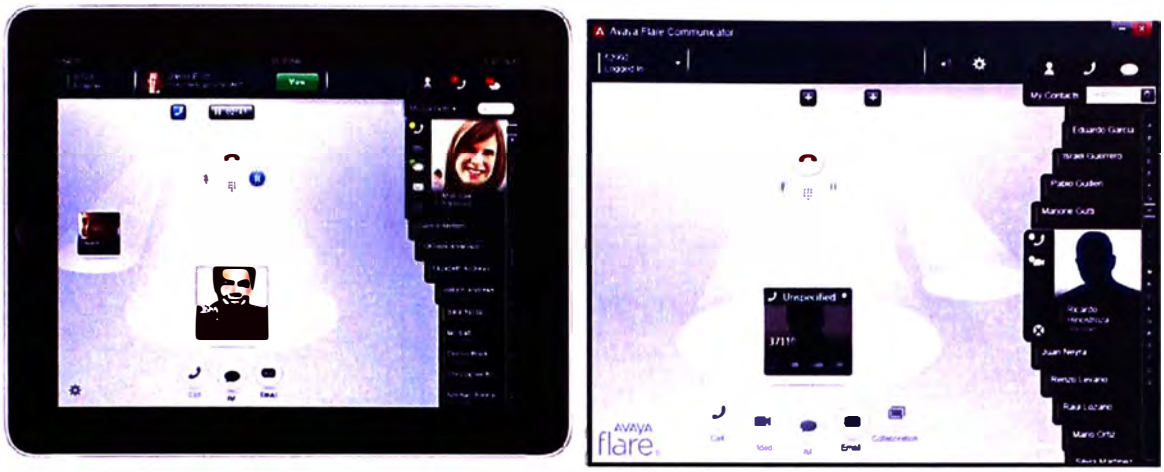


Figura 3.6 Avaya Flare Communicator para iPad y para Windows

c. Avaya Video Conference Systems 1000 Series

Avaya Video Conference Systems 1000 Series es una gama de cámaras de video para videoconferencias basadas de alta definición (1080p/720p) y bajo ancho de banda basadas en SIP. Estos equipos tienen una interface intuitiva que permite manejar fácilmente las llamadas de video de la misma forma que las llamadas de audio utilizando el plan numérico del Grupo Empresarial.

En este informe se van a utilizar las cámaras Avaya 1010, las cuales son cámaras de escritorio para que los usuarios puedan realizar sus llamadas de voz o de video (punto a punto), tienen enfoque estático y cuentan con micrófono incorporado. Las configuraciones y las órdenes para las llamadas se realizan con el control remoto del equipo. Adicionalmente tendremos las cámaras Avaya 1040, que son cámaras para Salas de Reuniones con enfoque motorizado y capaz de realizar zoom, además cuenta con un MCU (Multipoint Control Unit) de 4 puertos para atender a 4 usuarios a la vez en una misma pantalla.

Estos equipos se registran en la Plataforma Avaya Aura como si fueran una estación SIP más como cualquier otro anexo, esto es lo que simplifica las comunicaciones. Luego, toda configuración sobre las propiedades de la estación SIP de la cámara se hace desde la interface web del Avaya System Manager.

Figura 3.7 Avaya 1010 y Avaya 1040

CAPITULO IV
SOLUCION DEL PROBLEMA CON AVAYA AURA

4.1. Puesta en Servicio de Avaya Aura

A continuación se describe la puesta en servicio de los servidores que conforman la plataforma Avaya Aura:

4.1.1. Puesta en Servicio de Avaya Communication Manager

A continuación se describe la puesta en servicio del Avaya Communication Manager

a. Hardware para Avaya Communication Manager

Para poner en servicio el Avaya Communication Manager requerimos el siguiente servidor:

- Servidor: S8800, 1U Base
- CPU: 1 x E5620 2.4 Ghz 4-core
- Memoria RAM: 12GB
- Discos Duros: 3 discos duros de 146GB 10K
- Tipo de Raid: 5
- Tarjeta de Red Dual
- Fuente de Poder: 1 x 460 W

b. Instalación de Avaya Communication Manager

Lo primero que se debe realizar es instalar el software base System Platform en el servidor S8800, este proceso puede verificarse en el Anexo A. Una vez realizado esto desplegar la imagen de instalador de Avaya Communication Manager sobre el System Platform. Para el escenario que estamos describiendo utilizamos el CM_Simplex 6.1.0.0.2350 y lo instalaremos de la siguiente manera:

Ingresar al System Platform por consola web como admin.

Ingresar al campo Virtual Machine Management, y luego a Solution Template. Ahí seleccionaremos desde donde se realizará la instalación. En nuestro caso se instaló desde un DVD.

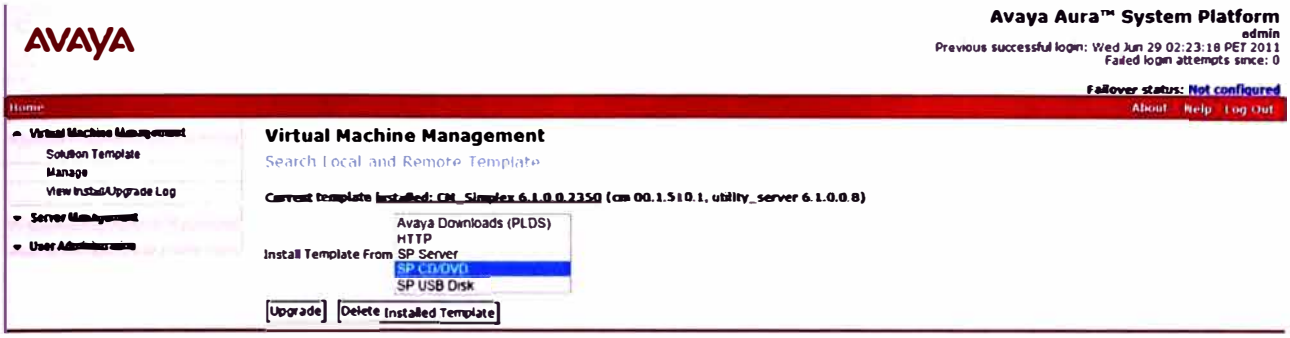


Figura 4.1

Se busca el archivo descriptor de la plantilla y se procede con la instalación. El proceso de instalación puede verse dentro de Virtual Machine Management, en View Install/Upgrade Log.

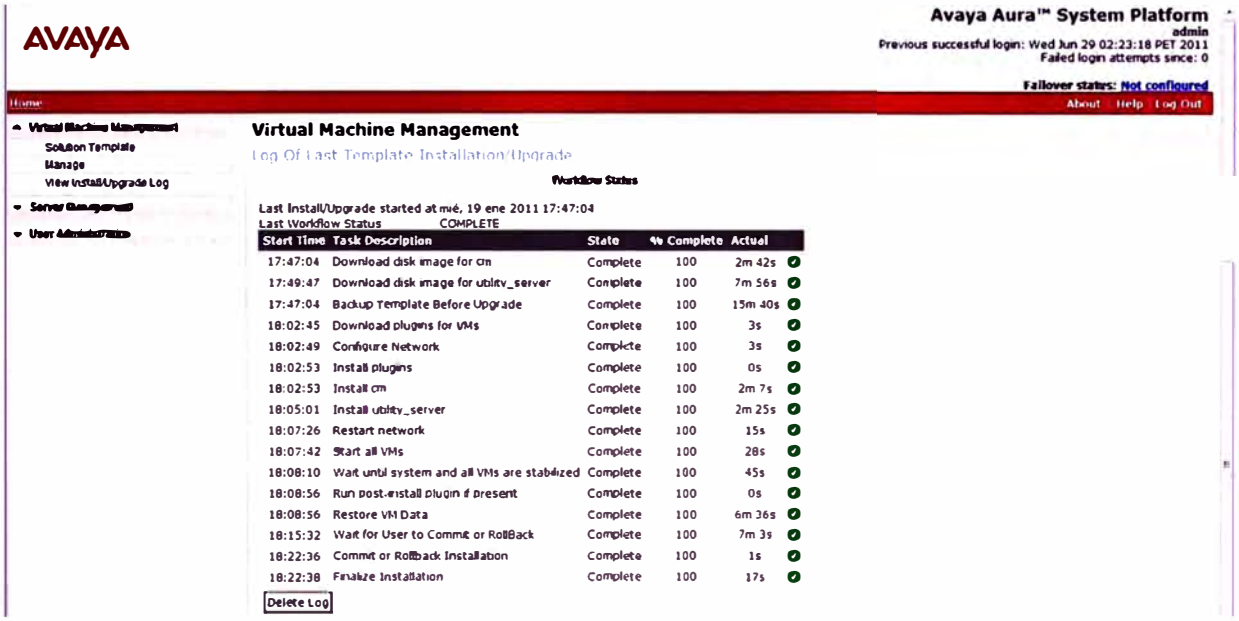


Figura 4.2

Luego se verifica el estado de la aplicación instalada. Dentro de Virtual Machine Management se ingresa a Manage y se elige la aplicación "cm".

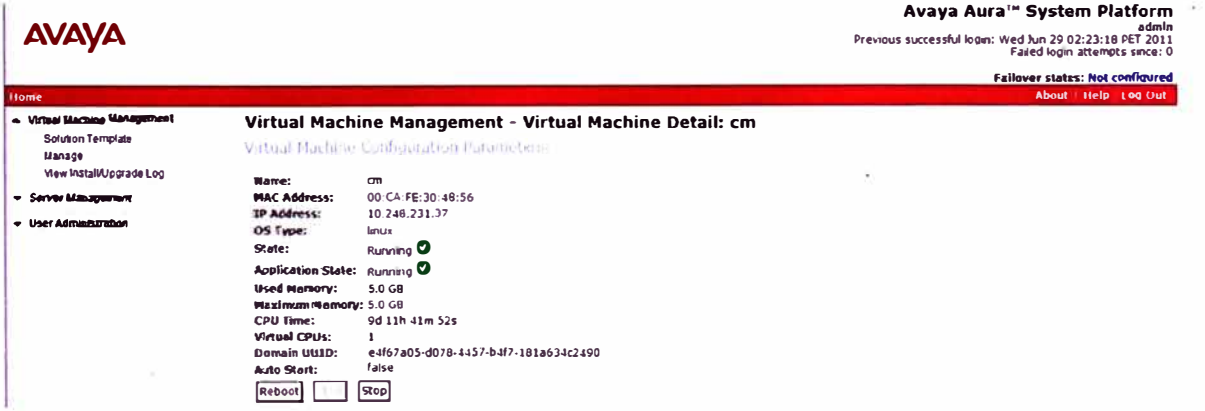


Figura 4.3

Finalmente se asignan los parámetros IP respectivos. En el apartado Server Management, en Network Configuration.

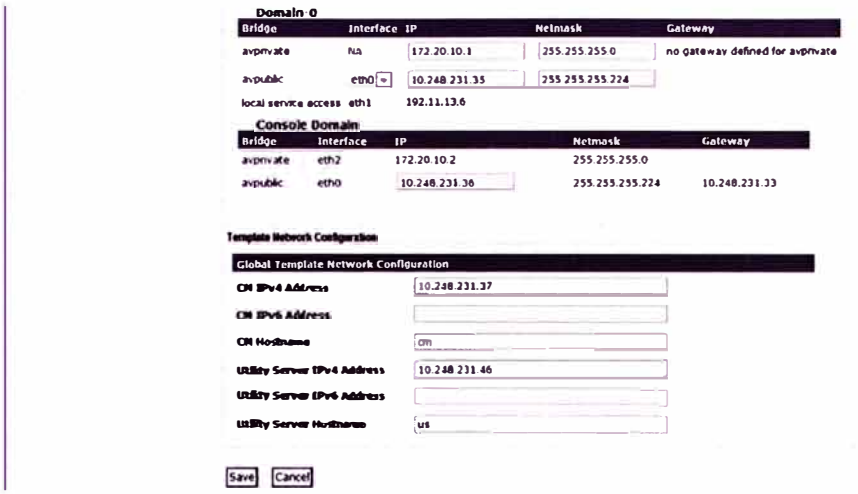


Figura 4.4

c. Configuración de Avaya Communication Manager

Para configurar el Avaya Communication Manager se utiliza la consola propietaria Avaya Site Administration, el cual debe estar instalado en una PC y se ingresan los comandos respectivos para configurar lo necesario:

Configurar la dirección IP del Avaya Communication Manager con el *comando add ip-interface procr*

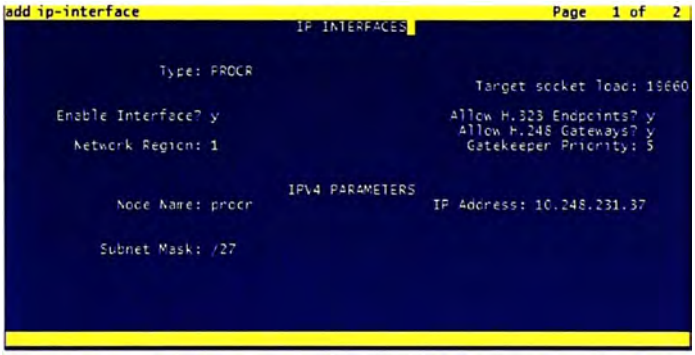


Figura 4.5 Comando add ip-interface procr

Se debe tomar en cuenta el Plan de Numeración que use el Grupo Empresarial y verificar que serie esté libre, si tomamos por ejemplo la serie 5XXXX para la plataforma, esta se declara con el comando *change uniform-dialplan*

Figura 4.6 Comando change uniform-dialplan

Declarar la serie 5XXXX para los anexos locales, el prefijo 80 para llamar a números externos y el prefijo 9 para hacer las llamadas hacia los anexos de las demás empresas del Grupo, con el comando *change dialplan analysis*

Figura 4.7 Comando change dialplan analysis

De igual manera, los prefijos 80 y 9 mencionados en el paso anterior deben ser declarados en los campos *Alternate Routing (AAR) Acces Code* y *Auto Route Selection (ARS) Acces Code* respectivamente con el comando *change feature-access-codes*

Figura 4.8 Comando change feature access-codes

Definir las Clases de Servicio para los anexos (COS) con el comando *change cos-group x* (x: Nro. de COS)

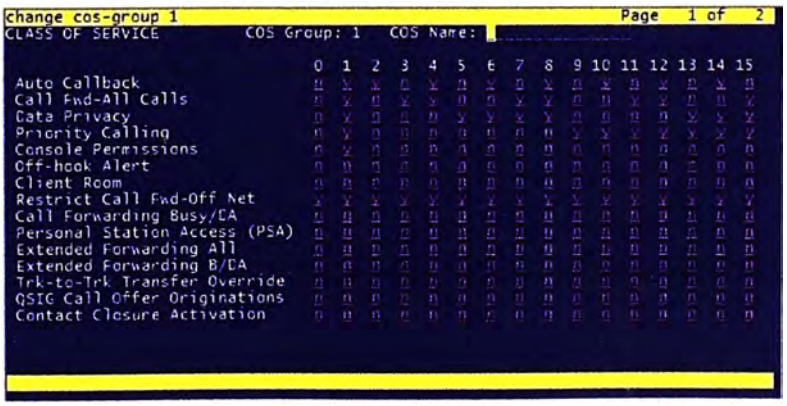


Figura 4.9 Comando change cos-group 1

Definir los niveles de restricción de llamadas para los anexos y códigos de autorización telefónicos (COR) con el comando *change cor x* (x: Nro. de COR)

Figura 4.10 Comando change cor 2

Verificar los parámetros del sistema brindados por personal de Avaya con el comando *display system-parameters customer-options*.

Figura 4.11 Comando display system-parameters customer-options

Configurar las listas de códecs para las comunicaciones en orden de preferencia con el comando *change ip-codec-set x* (x: Nro. de codec set)

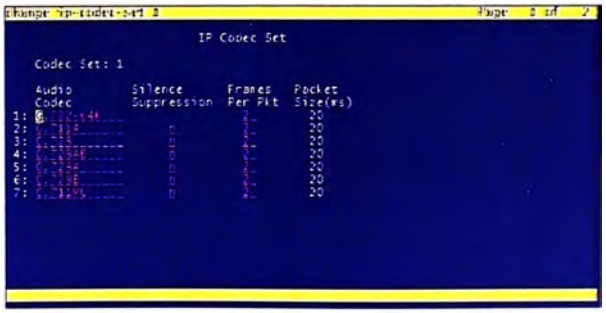


Figura 4.12 Comando display ip-codec-set 1

Configurar la región a la que pertenecerán los anexos de la plataforma, esta región determinará los recursos que utilizarán los anexos y se declara con *change ip-network región x* (x: Nro. de region)

Figura 4.13 Comando ip-network-region 1

Configurar el tratamiento de las llamadas con *system-parameters feature.*

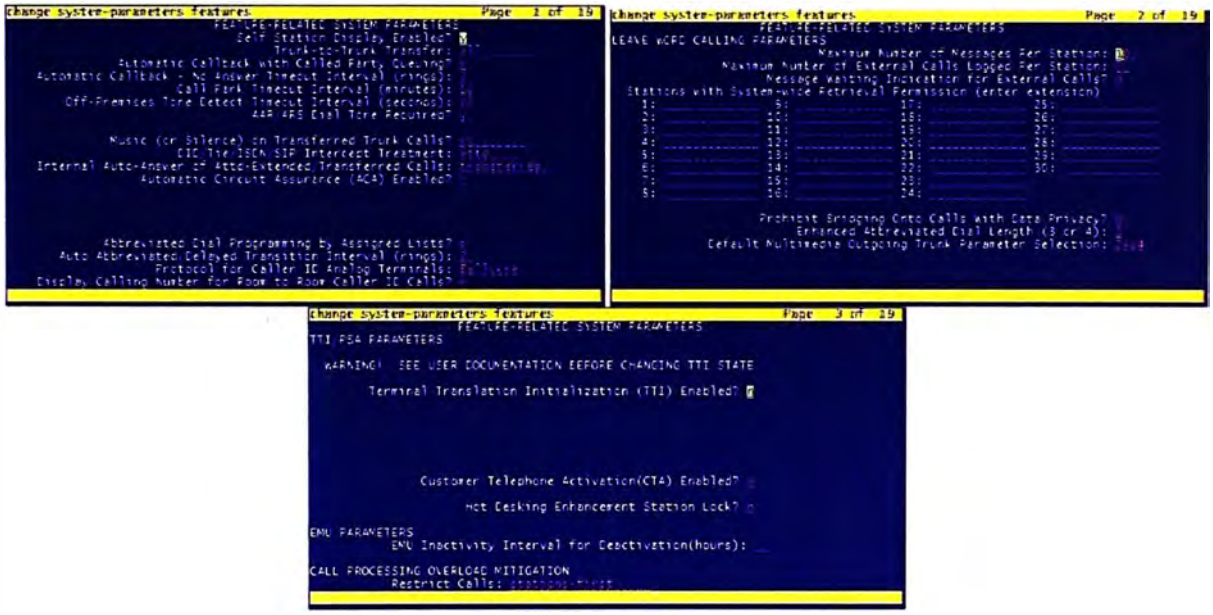


Figura 4.14 Comando change system-parameters features

Configurar las direcciones IP de los anexos para cada región con el comando *change ip-network-map*

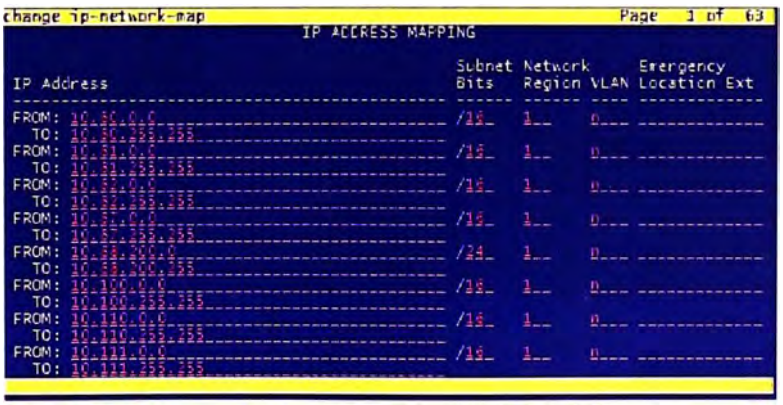


Figura 4.15 Comando change ip-network-map

Configurar el Gateway a utilizar para colocar los servicios PRI, anexos análogos y anexos digitales en caso hubieran, con el comando *add media-gateway x* (x: Nro. de Media Gateway)

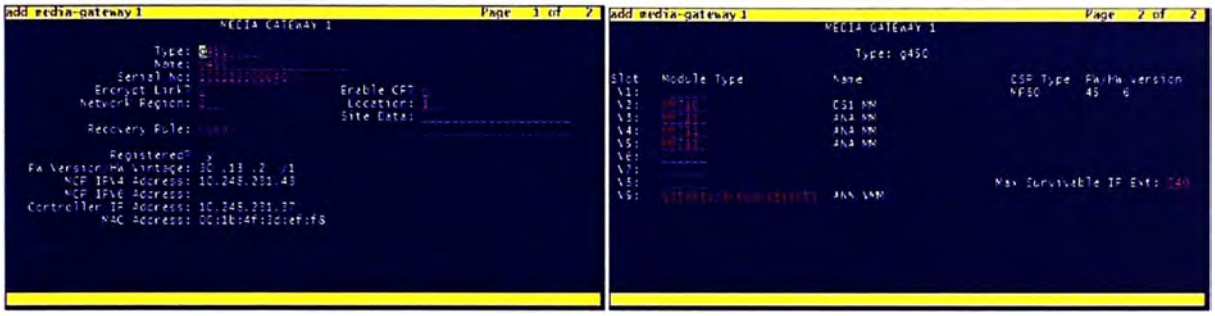


Figura 4.16 Comando add media-gateway 1

Configurar los anexos de los usuarios con el comando *add station xxxxx* (xxxxx: Nro. de anexo)

Figura 4.17 Comando add station 52992

Configurar los grupos de troncales con el comando *add trunk-group x* (x: Nro. de Grupo de Troncal)

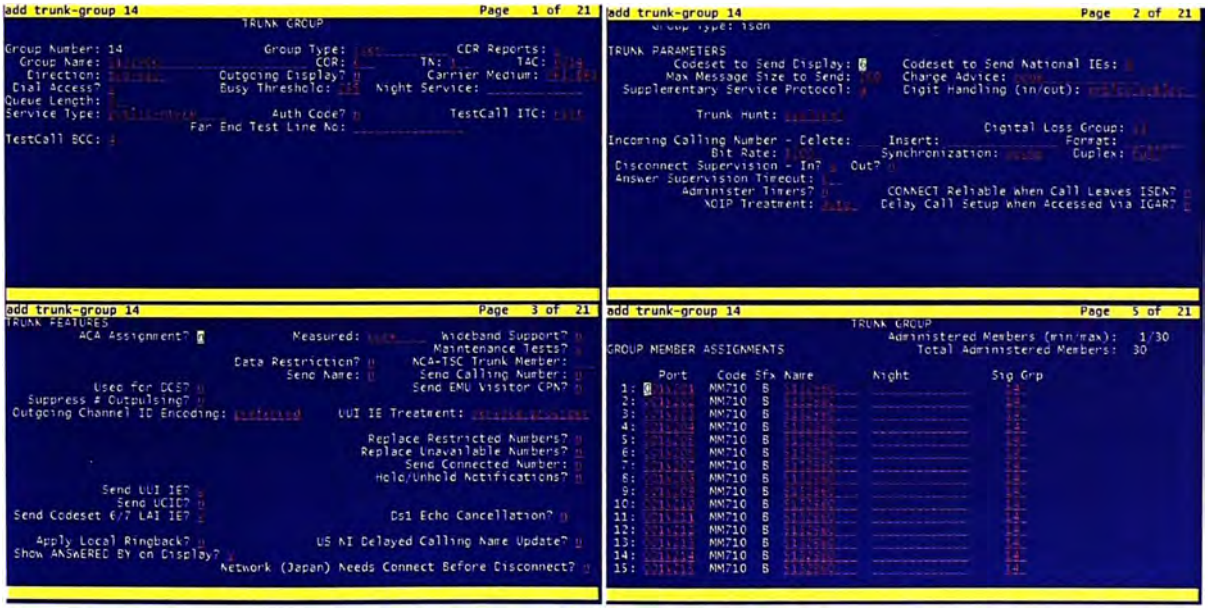


Figura 4.18 Comando add trunk-group 14

Configurar los grupos de señalización con el comando *add signalling group x* (x: Nro. de Grupo de Troncal)

Figura 4.19 Comando signaling-group 14

Ingresamos al explorador el URL https://ipadress e ingresamos con la cuenta *admin*, escogemos la opción Server (Maintenance) y nos abrirá una página en la que entraremos a la categoría Security y dentro de ella a Administrator Accounts. Aquí ingresaremos una cuenta SMGR para que el System Manager tenga control sobre el Communication Manager y pueda administrarlo.

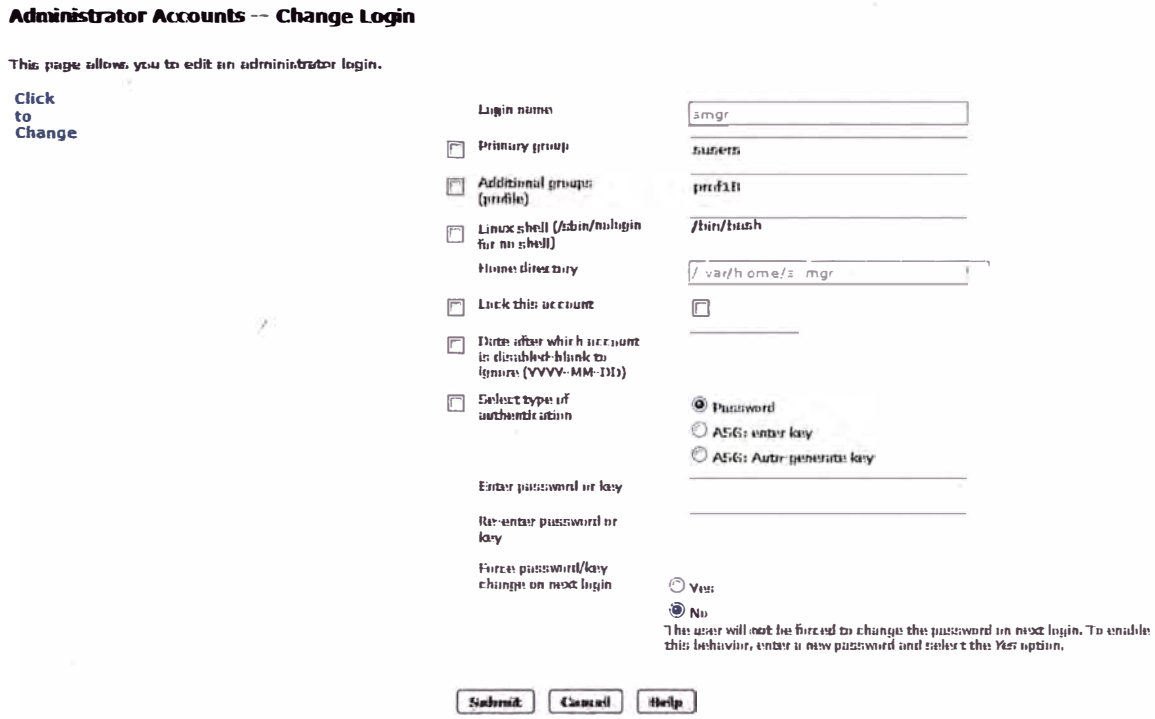


Figura 4.20 Creación de cuenta de administrador SMGR

4.1.2. Puesta en Servicio de Avaya System Manager

A continuación se describe la puesta en servicio del Avaya System Manager

a. Hardware para Avaya System Manager

Para poner en servicio el Avaya System Manager requerimos el siguiente servidor:

- Servidor: S8800, 1U Base
- CPU: 2 x E5620 2.4 Ghz 4-core
- Memoria RAM: 12GB
- Discos Duros: 3 discos duros de 146GB 10K
- Tipo de Raid: 5

- Tarjeta de Red Dual
- Fuente de Poder: 2 x 460 W

b. Instalación de Avaya System Manager

Lo primero que se debe realizar es instalar el software base System Platform en el servidor S8800, este proceso puede verificarse en el Anexo A. Una vez realizado esto desplegar la imagen de instalador de Avaya System Manager sobre el System Platform. Para el escenario que estamos describiendo utilizamos el Template_smgr 6.1.4.0 y lo instalaremos de la siguiente manera:

Ingresar al System Platform por consola web como admin.

Ingresar al campo Virtual Machine Management, y luego a Solution Template. Ahí seleccionaremos desde donde se realizará la instalación. En nuestro caso se instaló desde un DVD.

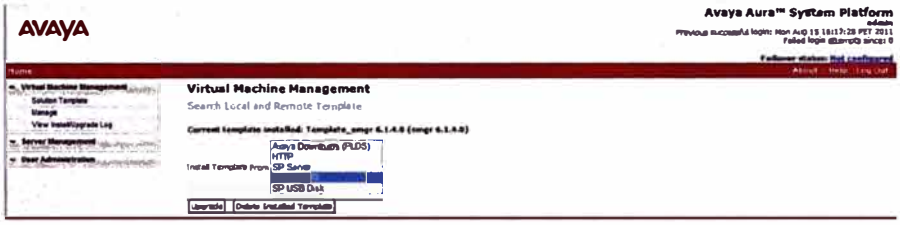


Figura 4.21

Se busca el archivo .ovf de la plantilla y se procede con la instalación. El proceso de instalación puede verse dentro de Virtual Machine Management, en View Install/Upgrade Log.

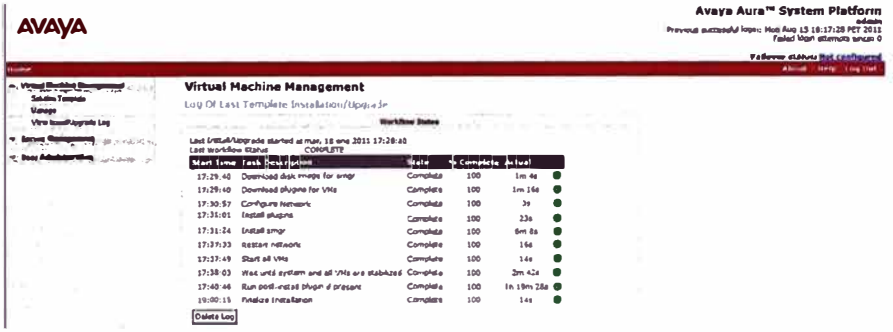


Figura 4.22

Finalmente se asignan los parámetros IP respectivos. En el apartado Server Management, en Network Configuration.

Figura 4.23

Luego se verifica el estado de la aplicación instalada. Dentro de Virtual Machine Management se ingresa a Manage y se elige la aplicación "SMGR".

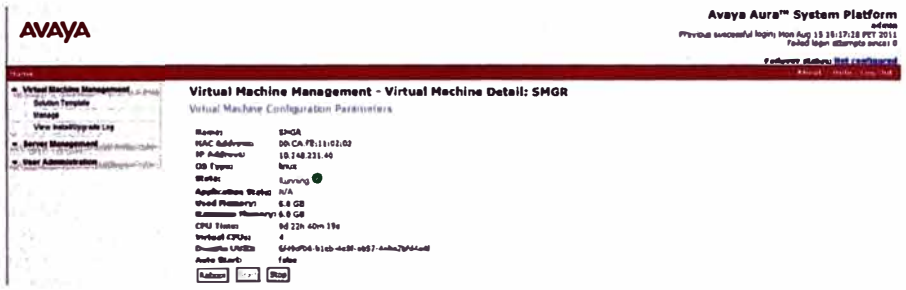


Figura 4.24

Verificamos el ingreso correcto al System Manager ingresando al explorador el siguiente URL https://ipadress colocando la IP que se haya configurado y luego comprobar el usuario y password configurados.

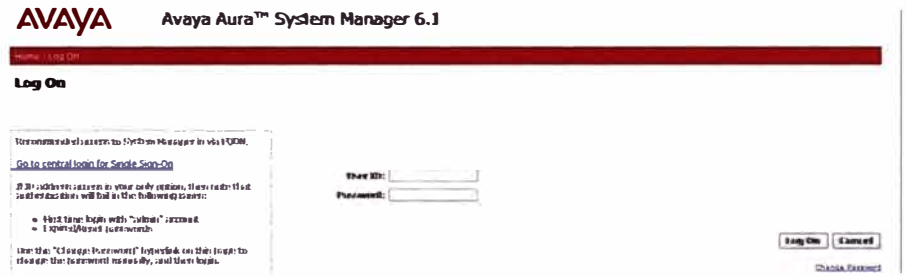


Figura 4.25

Una vez ingresemos al System Manager ingresamos a la categoría Inventory, luego en la opción Manage Elements dar "New" para ingresar los datos necesarios para que el System Manager converse con el Communication Manager, para esto se usa la cuenta de administrador SMGR que se creó en la sección anterior de este Informe.

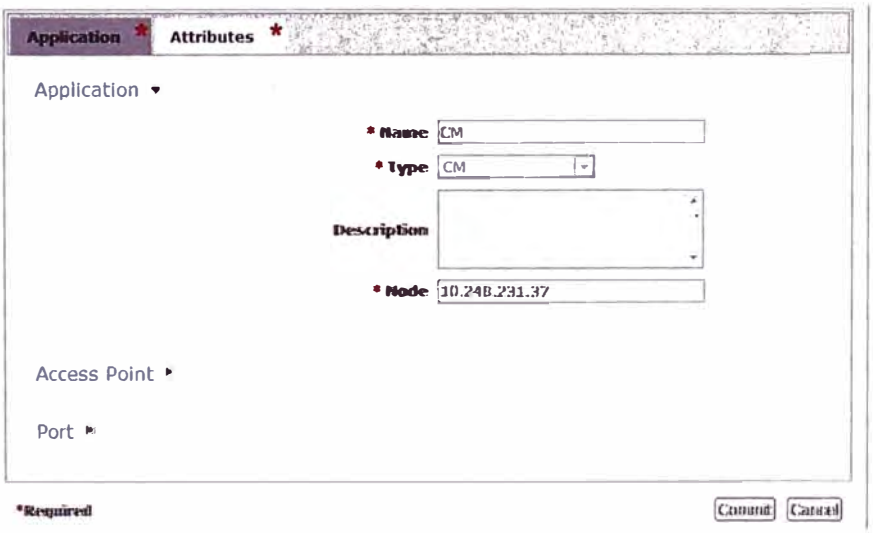


Figura 4.26

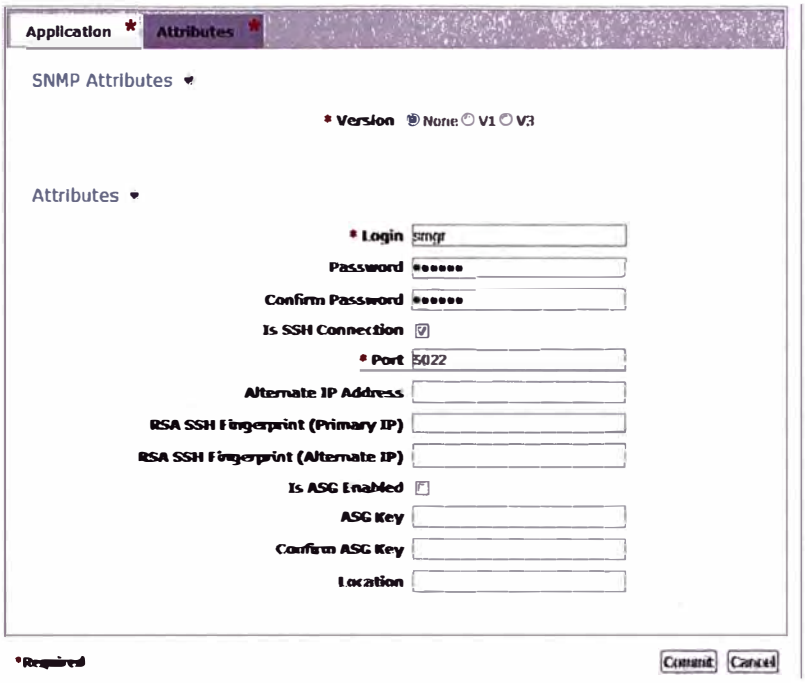


Figura 4.27

Una vez ingresemos al System Manager ingresamos a la categoría Security, luego en la opción Certificates debemos crear un Enrollment Password, el cual permitirá conversar al System Manager con el Session Manager

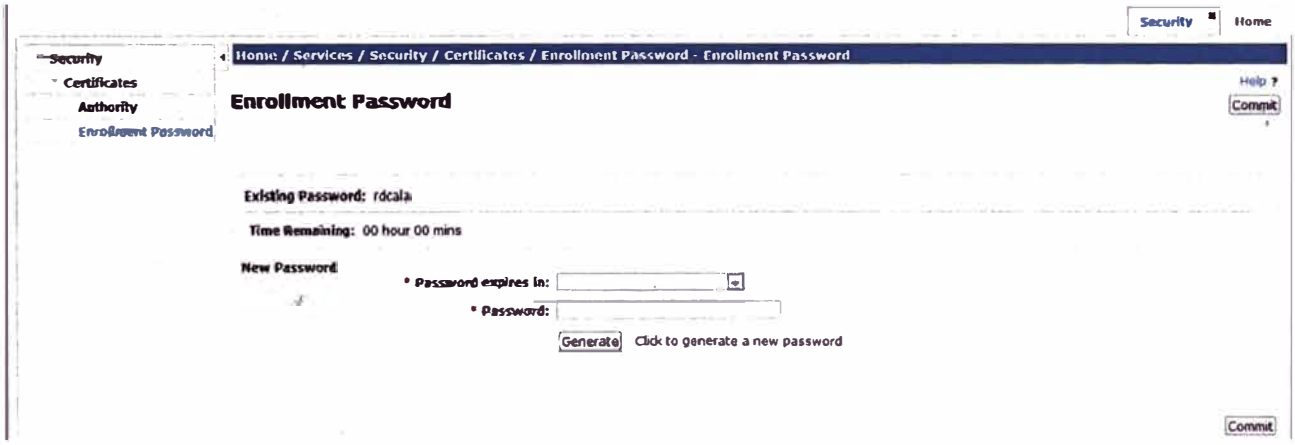


Figura 4.28

4.1.3. Puesta en Servicio de Avaya Session Manager

A continuación se describe la puesta en servicio del Avaya Session Manager

a. Hardware para Avaya Session Manager

Para poner en servicio el Avaya Session Manager requerimos el siguiente servidor:

- Servidor: S8800, 1U Base
- CPU: 2 x E5620 2.4 Ghz 4-core
- Memoria RAM: 12GB
- Discos Duros: 2 discos duros de 146GB 10K
- Tipo de Raid: 1

- Tarjeta de Red Dual
- Fuente de Poder: 2 x 460 W

b. Instalación de Avaya Session Manager

A diferencia de los demás servidores, el Avaya Session manager no es instalado sobre un System Platform sino más bien se configura directamente sobre un servidor con Red Hat Enterprise Linux 5.4, para esto se insertó un DVD con este software y se siguen los pasos intuitivamente hasta que termine dicha instalación y el servidor reinicie.

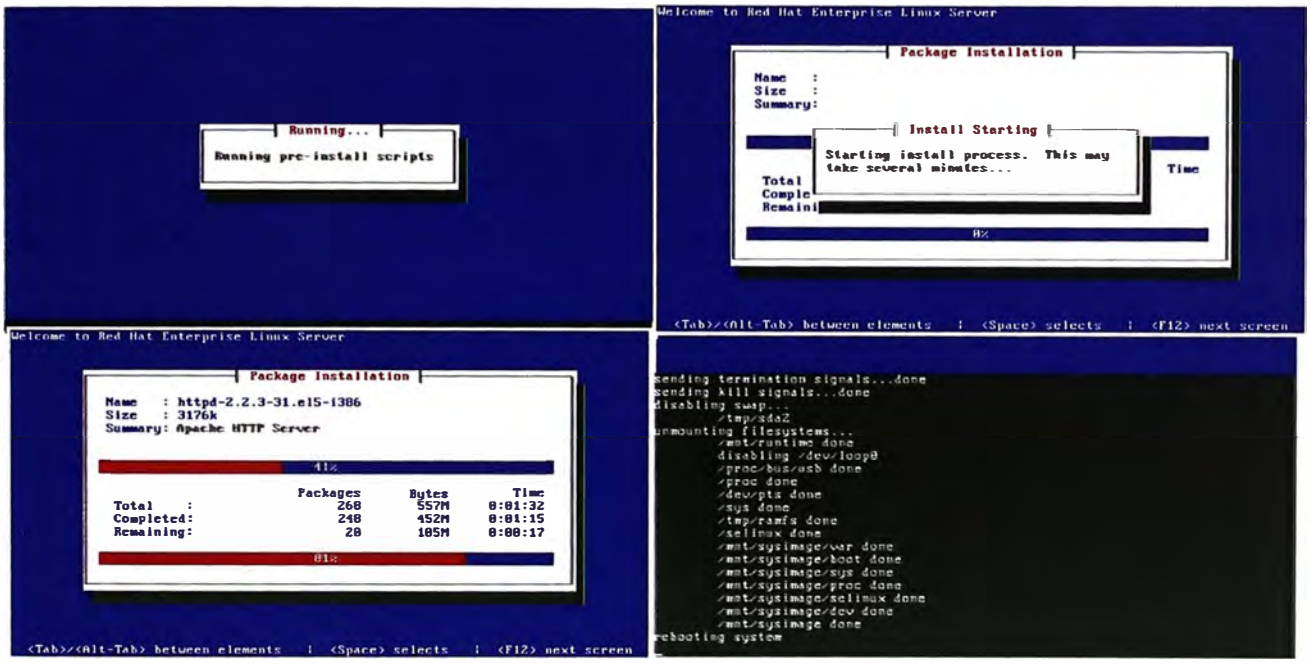


Figura 4.29

Teniendo el Red Hat instalado utilizamos el CD con el software del Session manager en el servidor. Ingresamos por consola Linux usando SSH y hacemos un login con cuenta craft o sroot. Una vez dentro de la consola usamos el comando ./SMnetSetup, el cual iniciará una serie de consultas sobre los parámetros de red para el Session Manager.

```
[craft@avaya-asm ~]$ ./SMnetSetup

Avaya Session Manager OS initial configuration

Current setting is found in enclosed with '[]'
Press ENTER to retain current setting
Enter 'none' to clear an optional setting

Enter server's hostname
[avaya-asm]: GM1-SM1

Enter server's IP address
[192.168.0.2]: 135.9.146.168

Enter netmask
[255.255.255.0]: 255.255.255.0

Enter gateway IP address
[]: 135.9.146.254

Enter network domain or 'none'
[localdomain]: global2.avaya.com

Enter primary DNS server IP address or 'none'
[]: 135.9.146.149
```

Figura 4.30

La consola nos pedirá confirmar los datos ingresados y luego iniciará un configurador.

Figura 4.31

Luego el instalador nos consultará por datos como la fecha, hora y por algún servidor NTP que exista en la red y que pueda ser utilizado.

Figura 4.32

Finalmente se nos consultará si deseamos crear alguna cuenta de administración y que confirmemos esta cuenta junto con los datos de DNS, NTP, dirección IP. Al dar Enter iniciará la primera parte de la instalación que durará aproximadamente 25 minutos y el servidor será reiniciado.

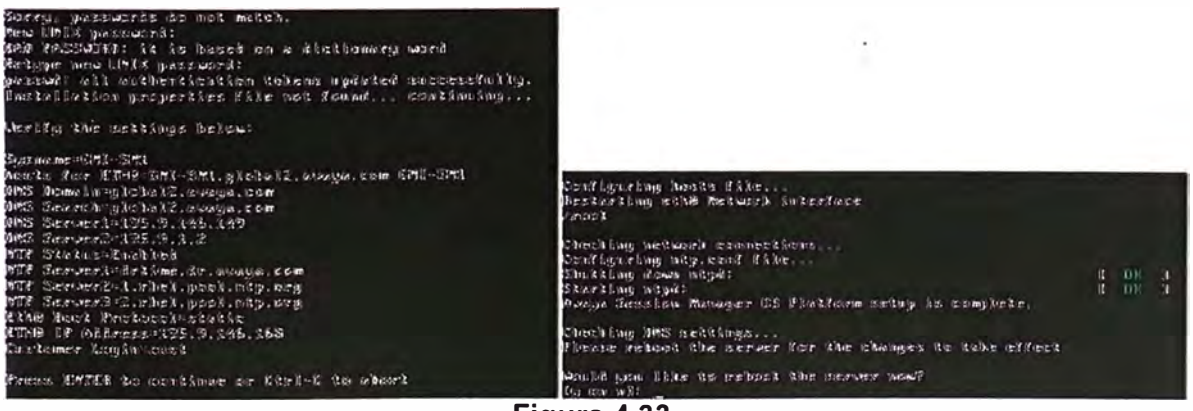


Figura 4.33

Una vez que el servidor haya reiniciado por completo podremos ingresar de nuevo a la consola Linux usando SSH con la cuenta sroot, buscaremos por comandos los archivos que contiene el CD de instalación.

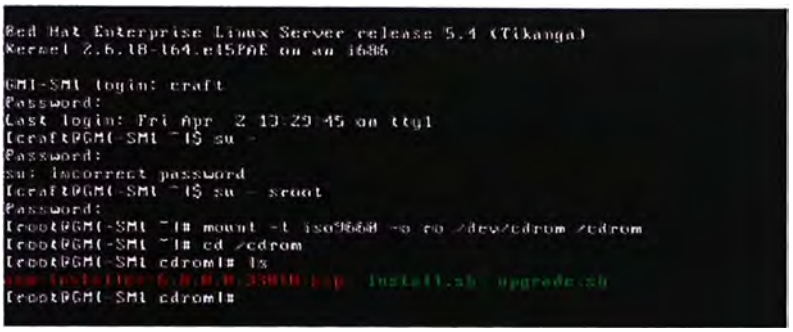


Figura 4.34

Tipeamos el comando ./install.sh y se inicia la segunda parte de la instalación corriendo una serie de procesos por cerca de 10 minutos. Terminado esto nos solicitará que confirmemos para pasar a la siguiente etapa.

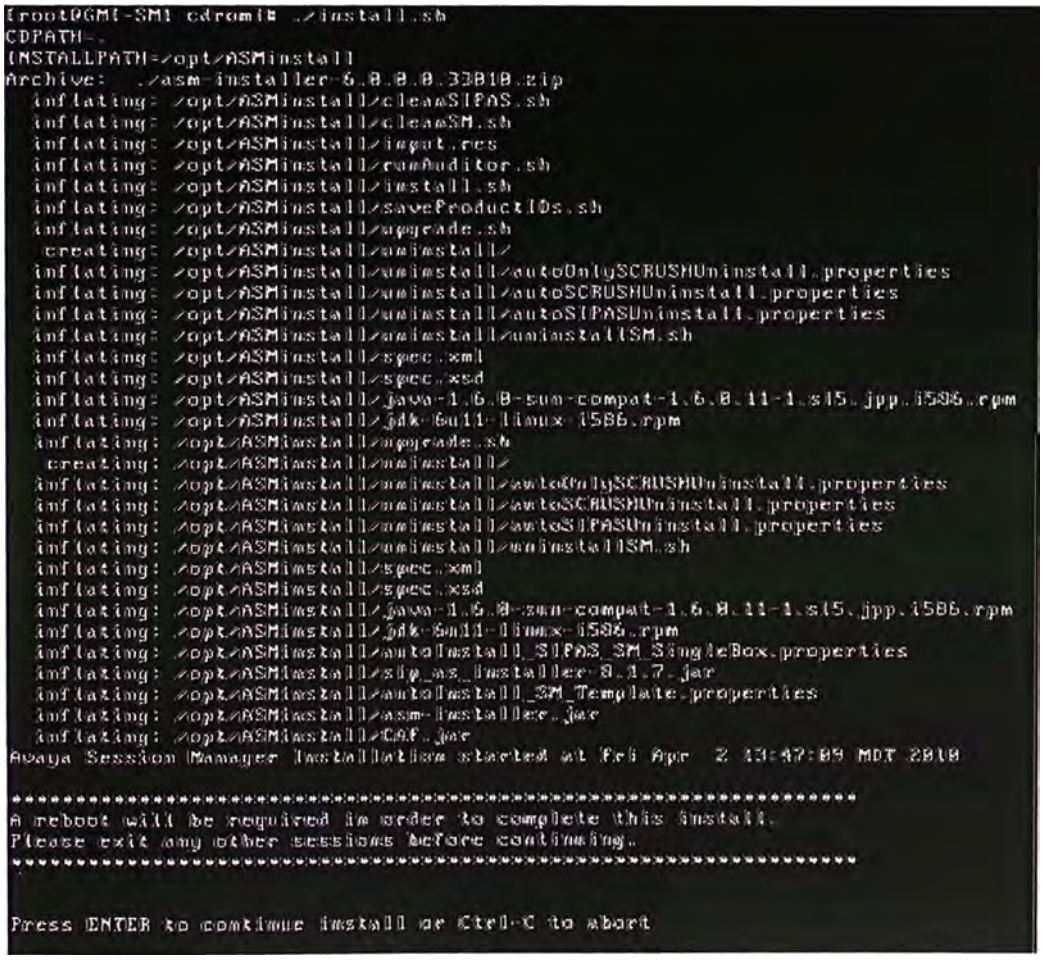


Figura 4.35

Luego nos consultarán por el System Manager que tendrá poder sobre el Session Manager, para lo cual ingresamos sus datos como IP y FQDN (si tuviera), damos Enter para confirmar.

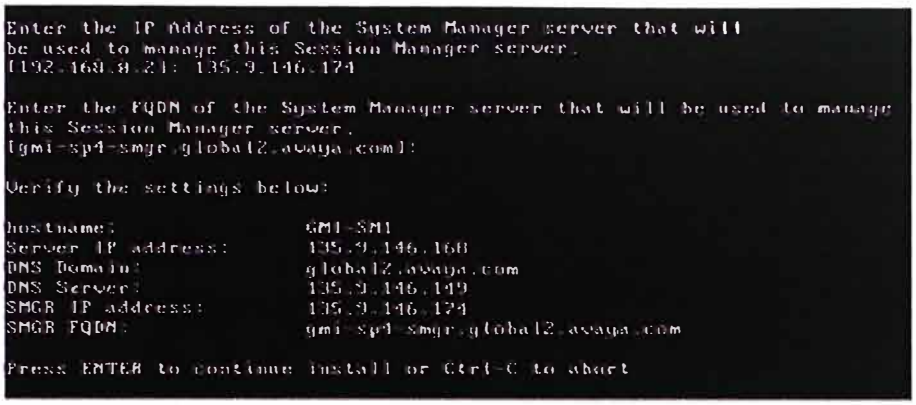


Figura 4.36

Finalmente nos solicitarán el Enrollment Password que configuramos en la sección anterior al instalar el System Manager. Una vez hecho esto el servidor reiniciará.

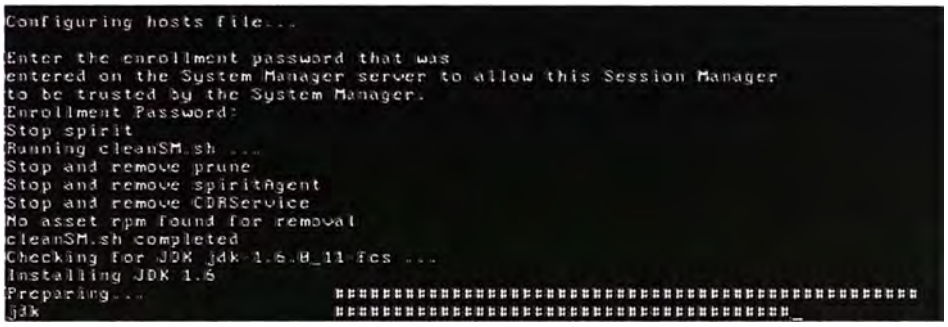


Figura 4.37

c. Inicialización de Avaya Session Manager

Ingresar al System Manager colocando en el explorador el URL https://ipadress/SMGR y utilizando la cuenta admin, ingresamos a la sección Routing, dentro ingresamos a la opción Domains e ingresamos el Dominio SIP sobre el cual trabajará la plataforma Aura.

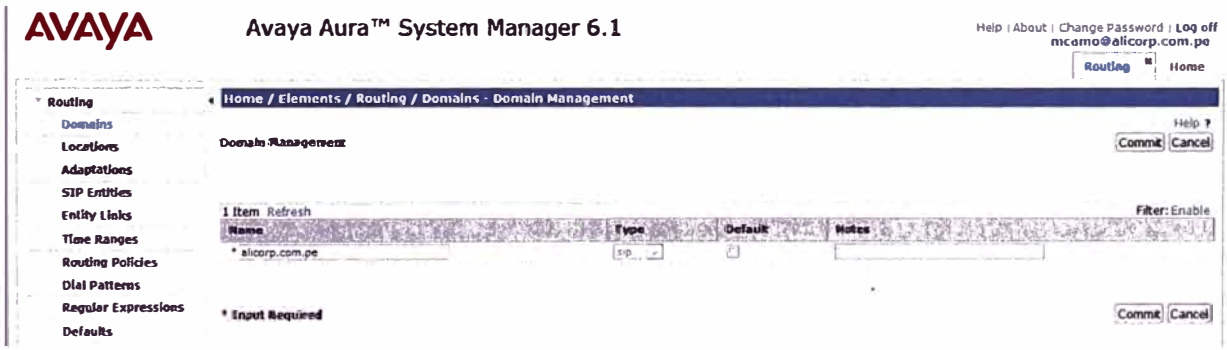


Figura 4.38

Luego, aún en la sección "Routing", encontramos el apartado "SIP Entities", escojemos la opción "New" para ingresar los datos de las entidades SIP que tenemos hasta el momento como el Communication Manager y su Mensajería de Voz, el Session Manager, la central CS1000 que servirá de comunicación entre la plataforma Aura y la Red Corporativa de Grupo, en este caso una CS1000 release 6.0.

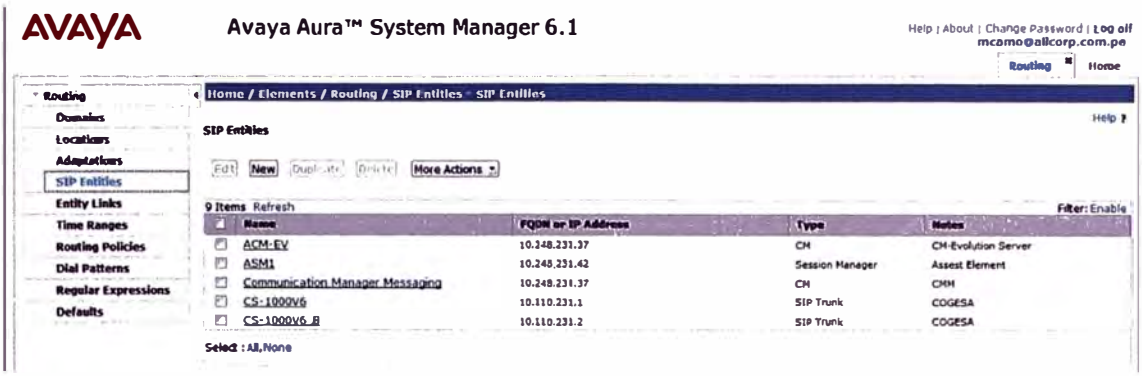


Figura 4.39

Luego, aún en la categoría "Routing", ingresamos a la opción "Entity Links", escojemos la opción "New" para ingresar los datos que describen la comunicación entre Avaya Session Manager y las entidades descritas en el paso anterior.

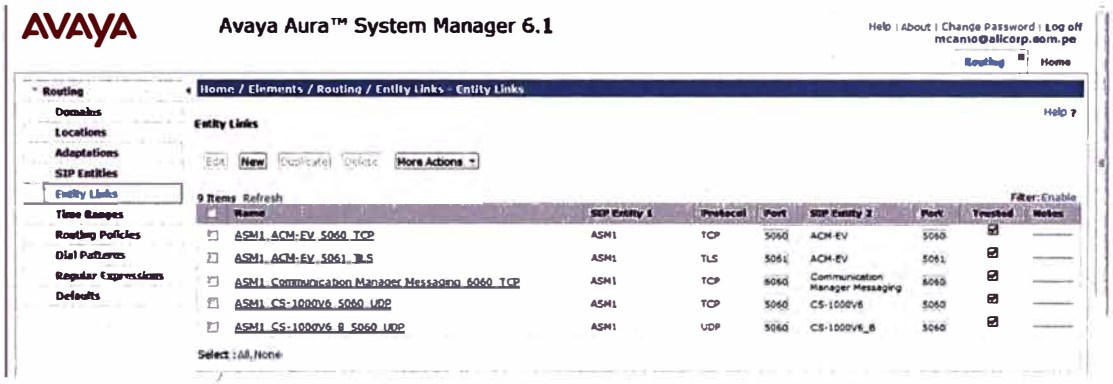


Figura 4.40

Luego retornamos al menú principal del System Manager y entramos a la categoría Session Manager, dentro de la cual tenemos la opción "Session Manager Administration", y dentro de esta vemos el campo "Session Manager Instances" al que le damos la opción "New" para ingresar determinados parámetros del Session Manager para que el System Manager pueda administrarlo correctamente.

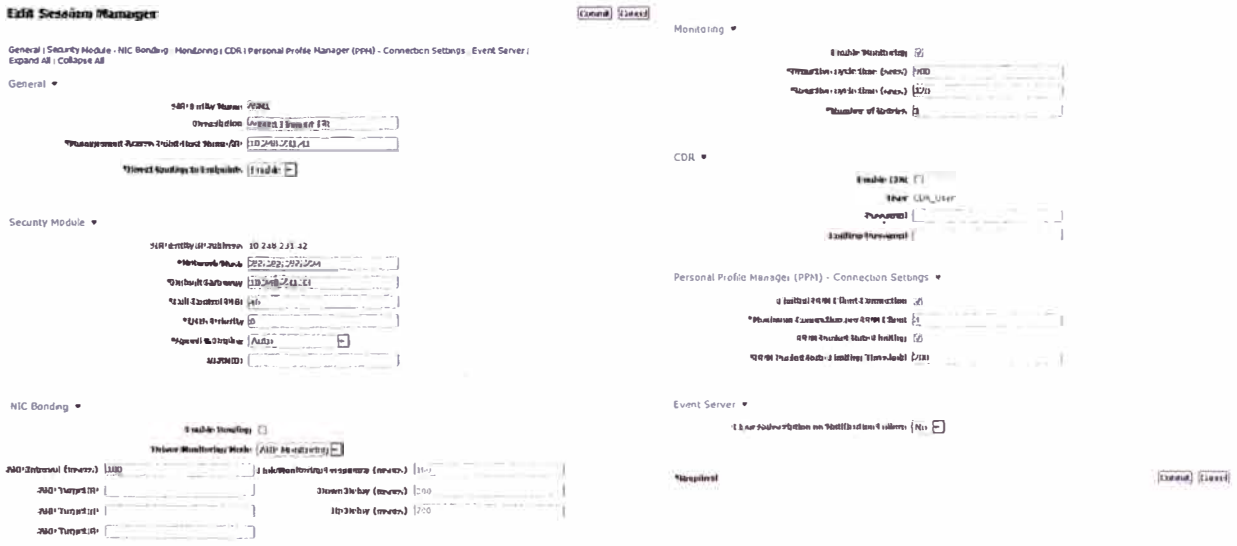


Figura 4.41

4.1.4. Puesta en Servicio de Avaya Presence Services

A continuación se describe la puesta en servicio del Avaya Presence Services

a. Hardware para Avaya Presence Services

Para poner en servicio el Avaya Session Manager requerimos el siguiente servidor:

- Servidor: IBM x3650 M3, 2U Base
- CPU: 2 x E5507 2.66 Ghz 4-core
- Memoria RAM: 7 x 4GB DDR3 1333Mhz
- Discos Duros: 5 discos duros de 146GB 15K
- Tipo de Raid: 5
- Tarjeta de Red Dual
- Fuente de Poder: 1 x 675 W redundante

b. Instalación de Avaya Presence Services

Lo primero que se debe realizar es instalar el software base System Platform en el servidor x3650 M3, este proceso puede verificarse en el Anexo A. Una vez realizado esto desplegar la imagen de instalador de Avaya Presence Services sobre el System Platform. Para el escenario que estamos describiendo utilizamos el Template_PS 06.01.00.00.03 y lo instalaremos de la siguiente manera:

Ingresar al System Platform por consola web como *admin*.

Ingresar al campo Virtual Machine Management, y luego a Solution Template. Ahí seleccionaremos desde donde se realizará la instalación. En nuestro caso se instaló de manera interna luego de subir el template al servidor, escogemos la opción "SP Server".

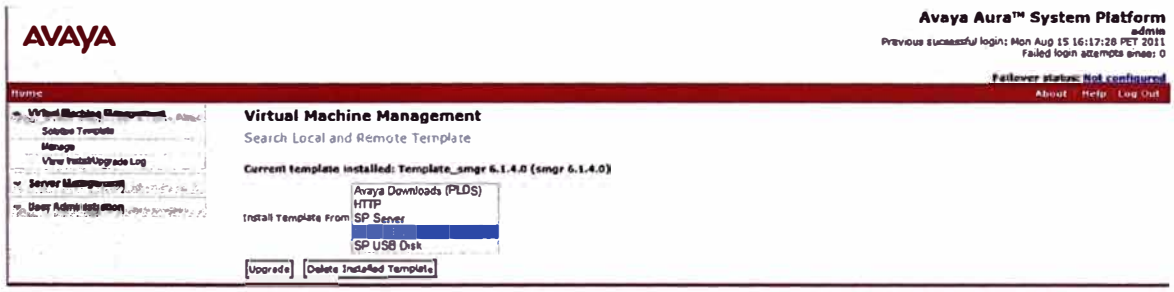
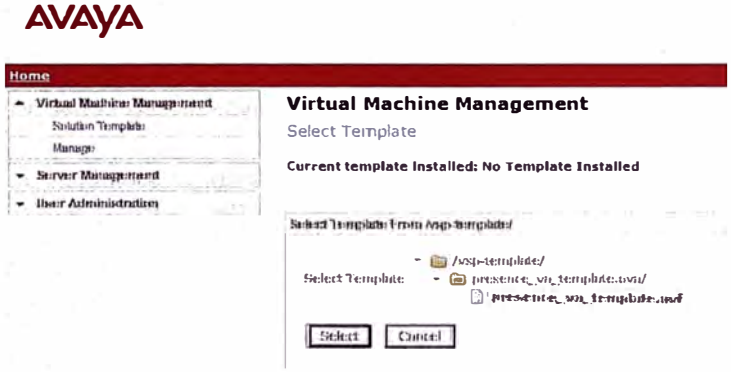


Figura 4.42

Se busca el archivo .ovf de la plantilla y se procede con la instalación.



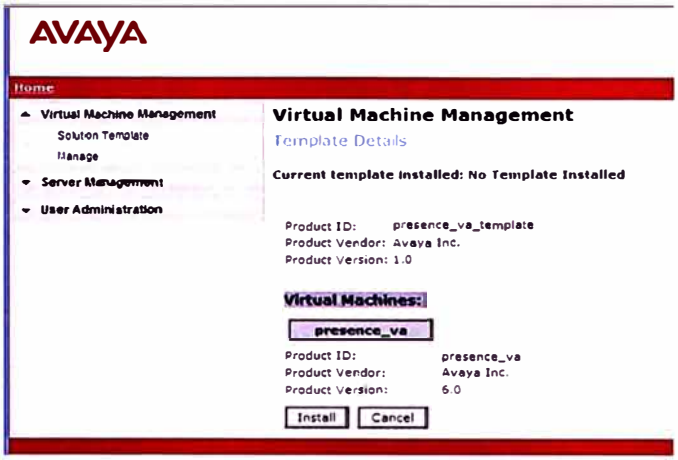


Figura 4.43

Se configuran los parámetros de red.

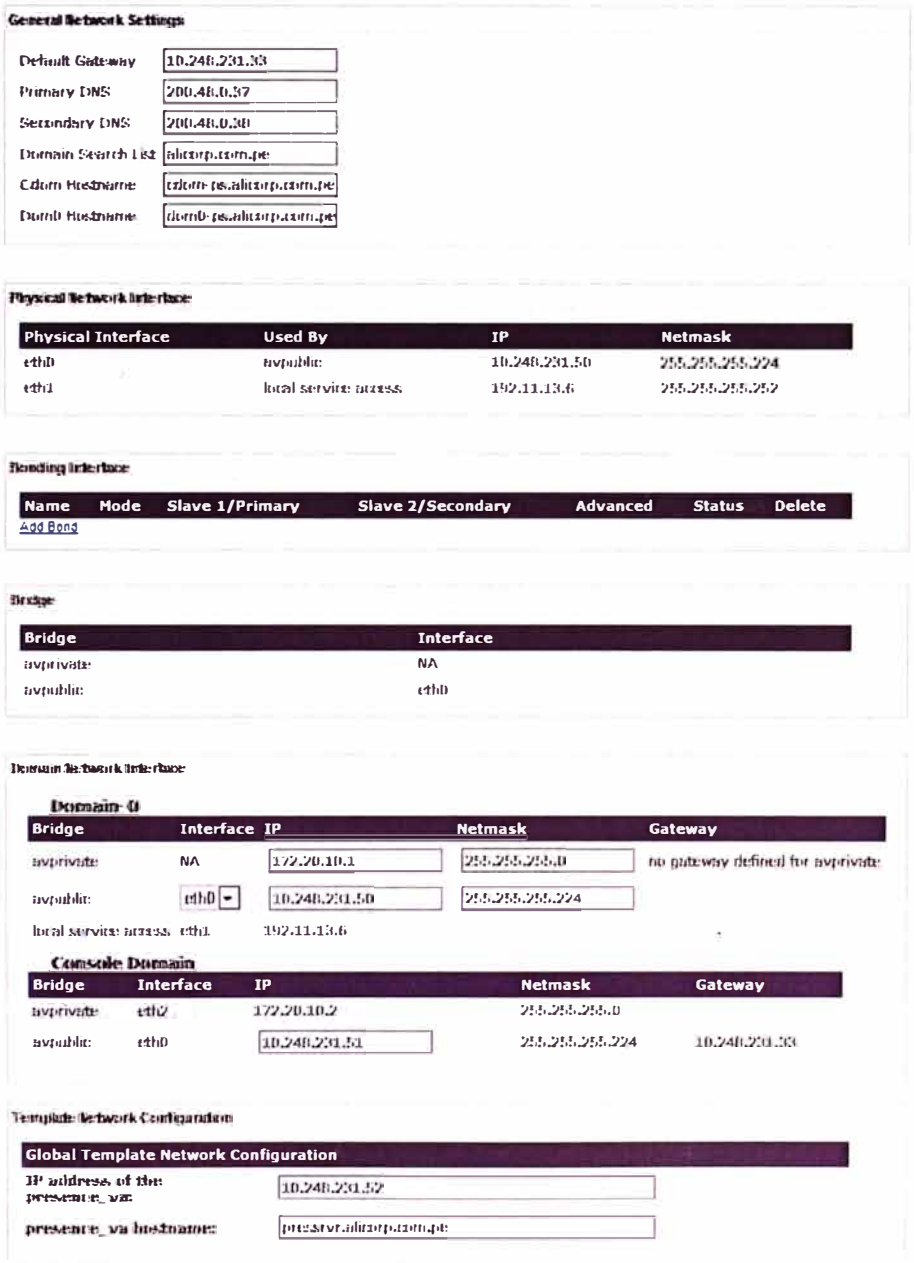


Figura 4.44

El proceso de instalación puede verse dentro de Virtual Machine Management, en View Install/Upgrade Log.

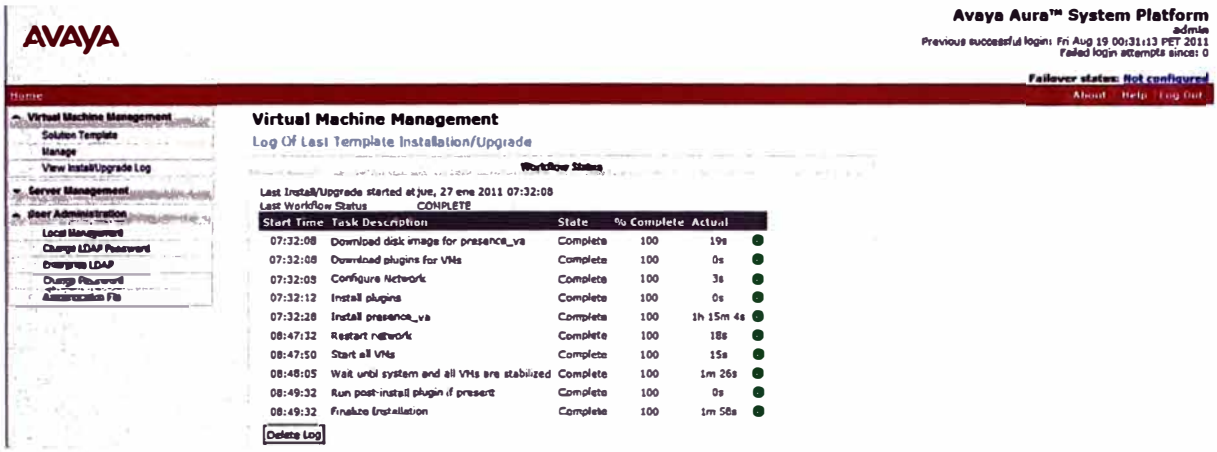


Figura 4.45

Luego se verifica el estado de la aplicación instalada. Dentro de Virtual Machine Management se ingresa a Manage y se elige la aplicación "PS".

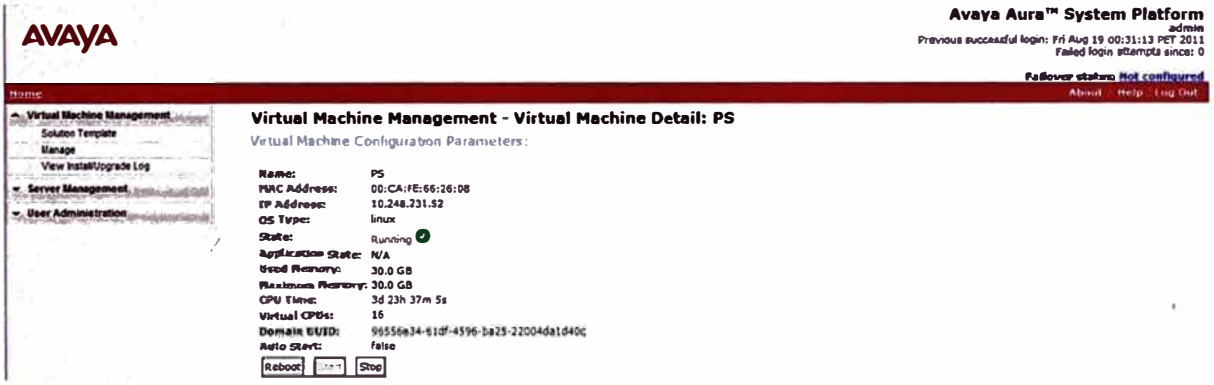


Figura 4.46

Verificamos el ingreso correcto al Presence Services ingresando al explorador el siguiente URL https://ipadress colocando la IP que se haya configurado y luego comprobar el usuario y password configurados.

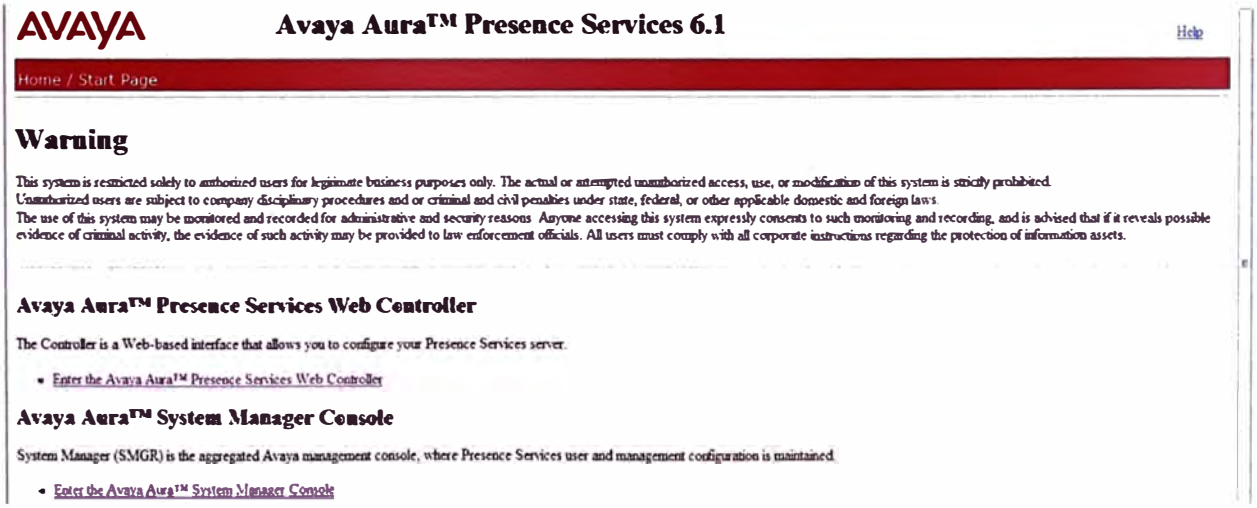


Figura 4.47

c. Inicialización de Avaya Presence Services

Ingresamos a la administración web del Avaya Presence Services y elegimos la vista de configuración Avanzada. Dentro del área Router vemos el campo "Global router settings", a lo cual escojemos la acción "edit". En la parte baja, en "Mutually trusted TLS Hostnames" se debe agregar la dirección IP del Avaya Session Manager.

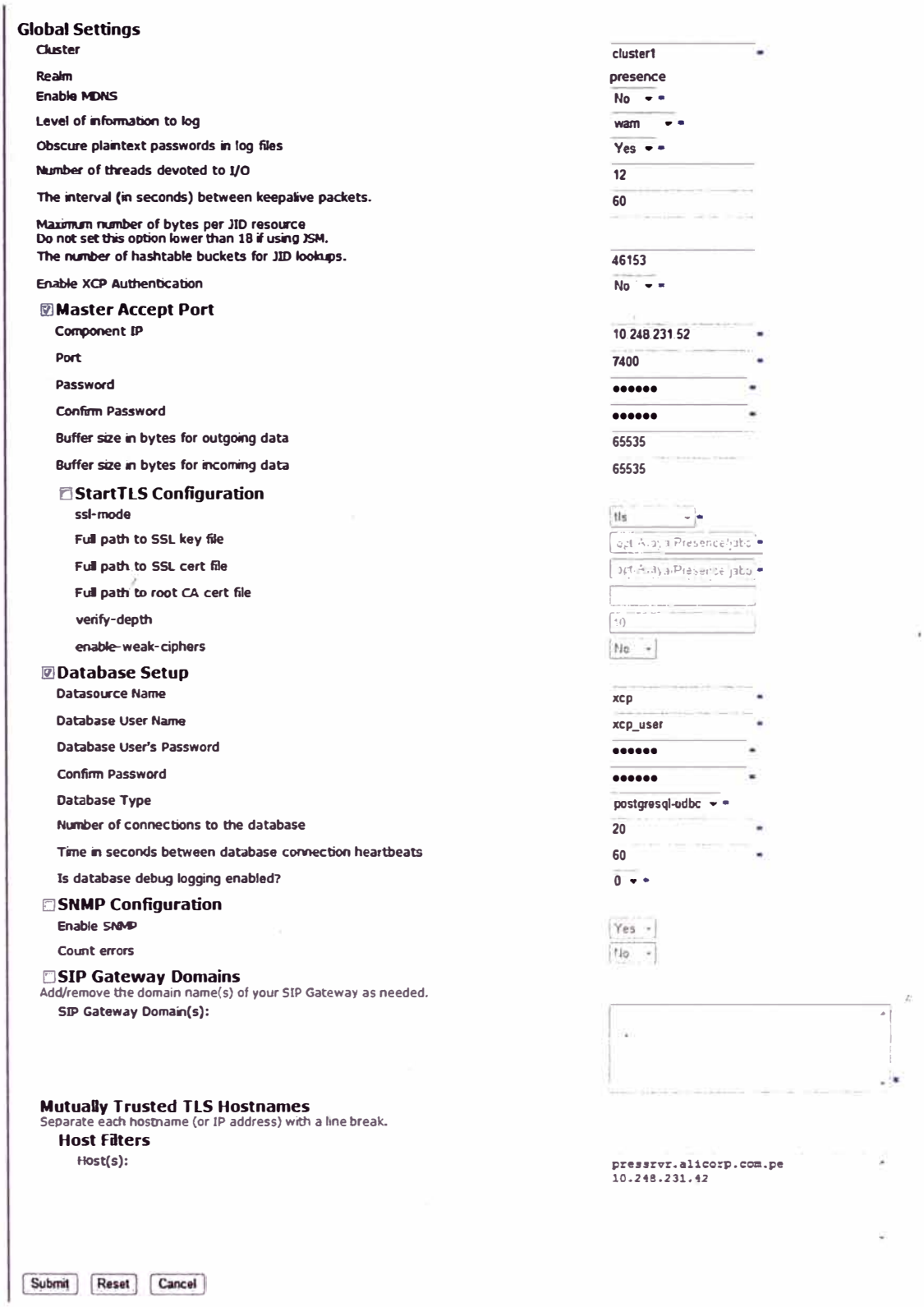


Figura 4.48

Ingresamos al System Manager por consola web y en la categoría "Routing" encontramos el apartado "SIP Entities", escogemos la opción "New" para ingresar los datos del Avaya Presence Services que ya tenemos instalado.

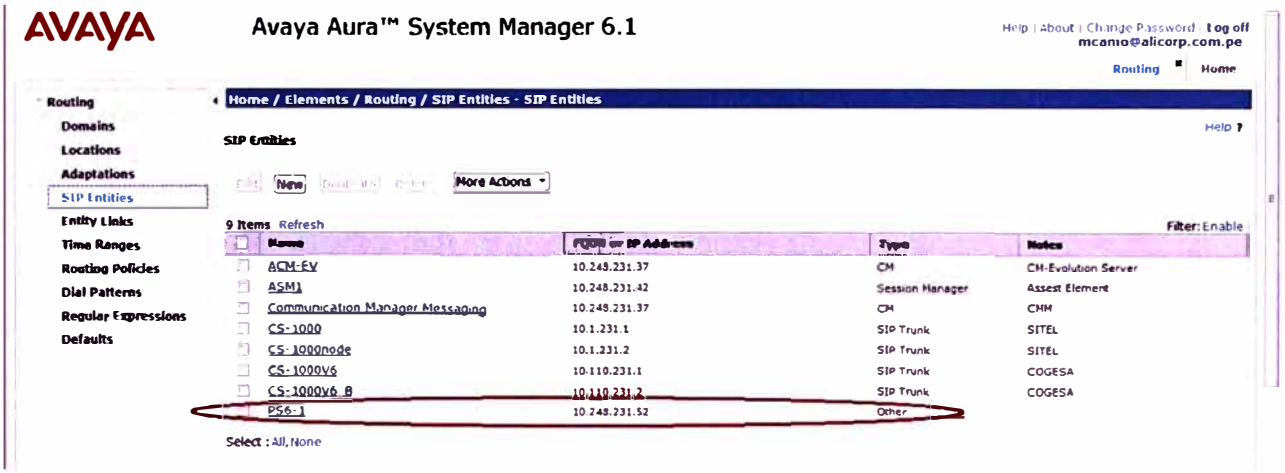


Figura 4.49

Luego, aún en la categoría "Routing del System manager, ingresamos al apartado "Entity Links", escogemos la opción "New" para ingresar los datos que describen la comunicación entre Avaya Session Manager y Avaya Presence Services.

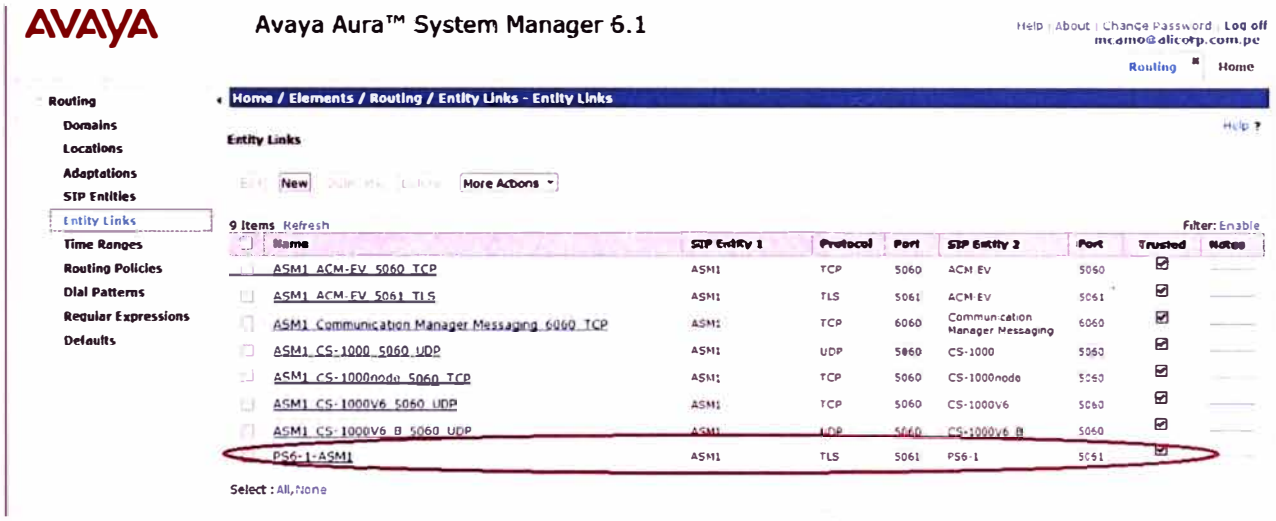


Figura 4.50

Después de esto hay que habilitar algunos módulos de presencia para Session Manager, para esto ingresamos a la consola web del Presence Services de nuevo con la vista de configuración Avanzada, dentro del área "Routing" elegimos la opción "edit" para el campo "Presence Session Manager", dentro debemos habilitar los módulos mostrados en la figura, además se debe habilitar la opción "SIP URI Mapping Configuration" y en la parte de "Send ID Mapping" debemos colocar "yes".

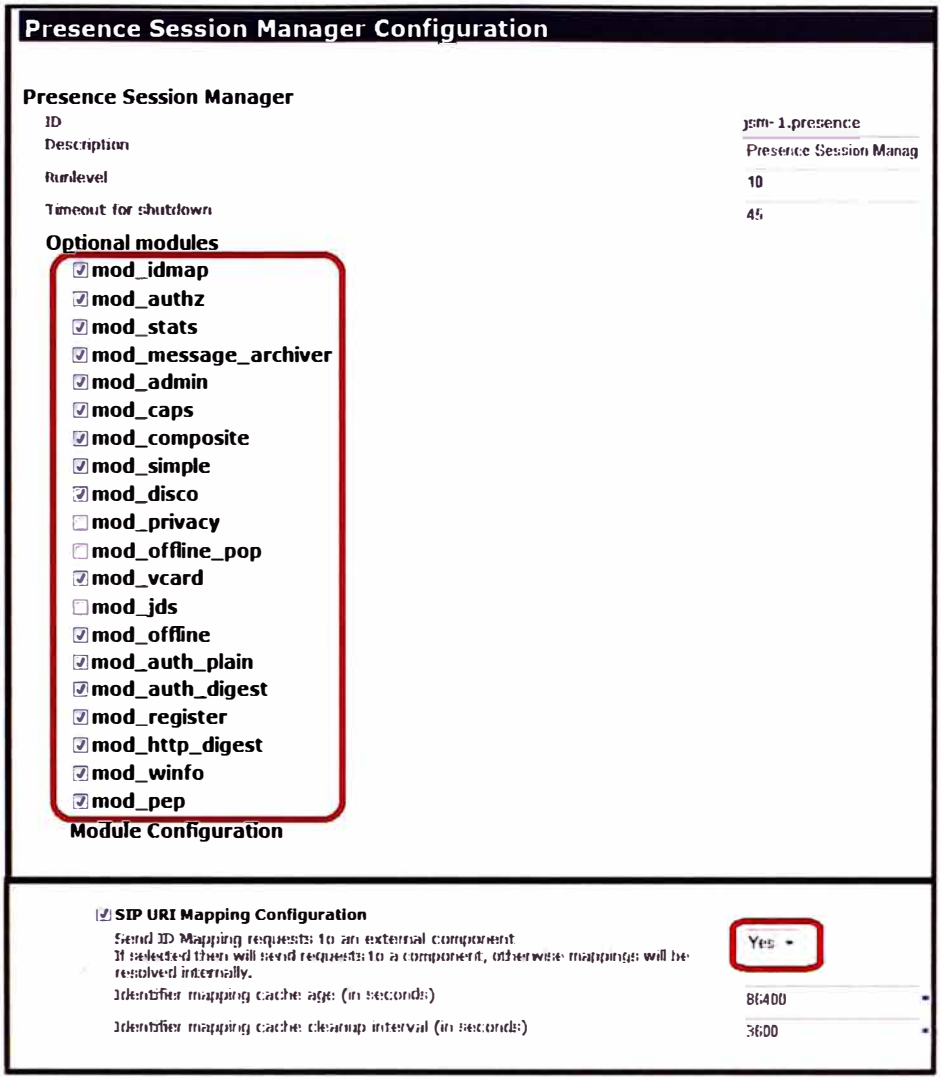


Figura 4.51

Podemos verificar el correcto funcionamiento de Presence Services ingresando a la consola web de System Manager, en la categoría "Inventory", luego entramos a la opción "Manage Elements" en donde deberíamos ver una entidad del tipo PS, y si ingresamos a ella y una vez dentro podemos dar clic al botón "Show" para ver el status de esa aplicación, la cual debería ser "Enabled"

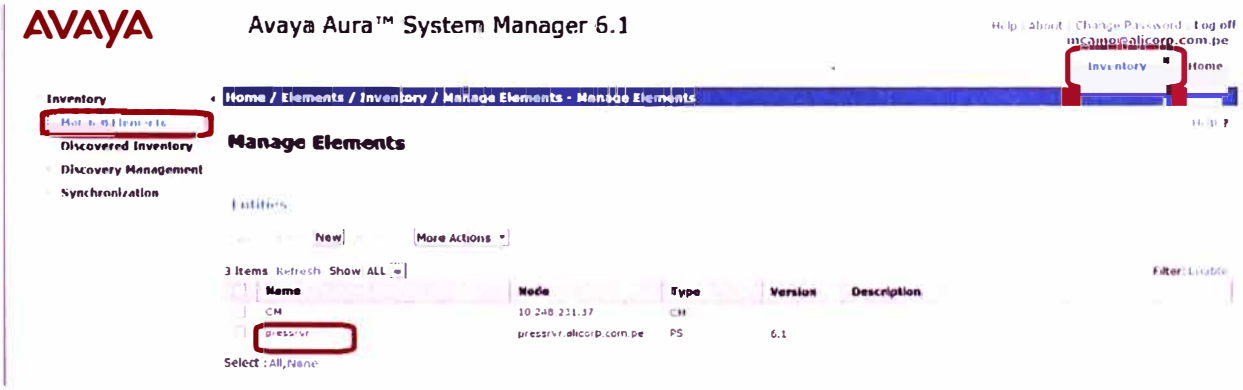


Figura 4.52

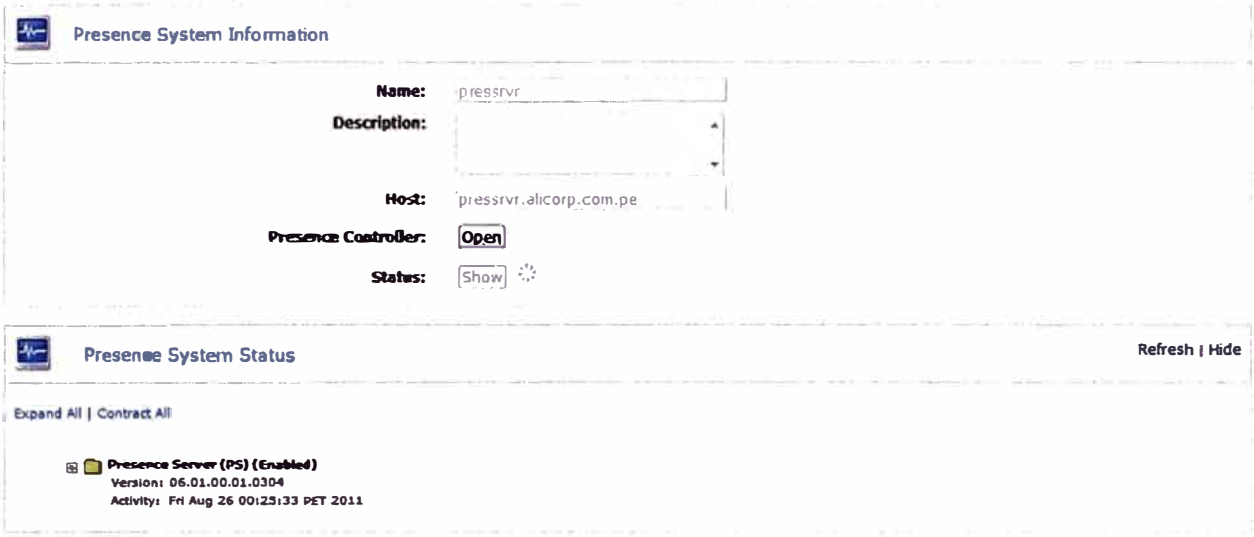


Figura 4.53

Ahora para agregar presencia a los user del System Manager debemos ingresar por su consola web a la categoría "User Management", dentro de ella entramos a la opción "Manage Users", elegimos al usuario que queremos habilitar presencia y damos la opción "Edit", al ver el perfil del usuario ingresamos a la opción "Contacts" para ver los contactos asociados al usuario elegido, editamos cualquiera de sus contactos y nos aseguramos de marcar la casilla "Presence Buddy", para confirmar la edición hacemos clic en el botón "Add" y luego para salir del perfil del usuario elegido damos clic en el botón "Commit". En la figura vemos que dentro del perfil del usuario aalvaa@alicorp.com.pe se edita el contacto Cam, Mikhail que tiene asociado para habilitar su presencia.

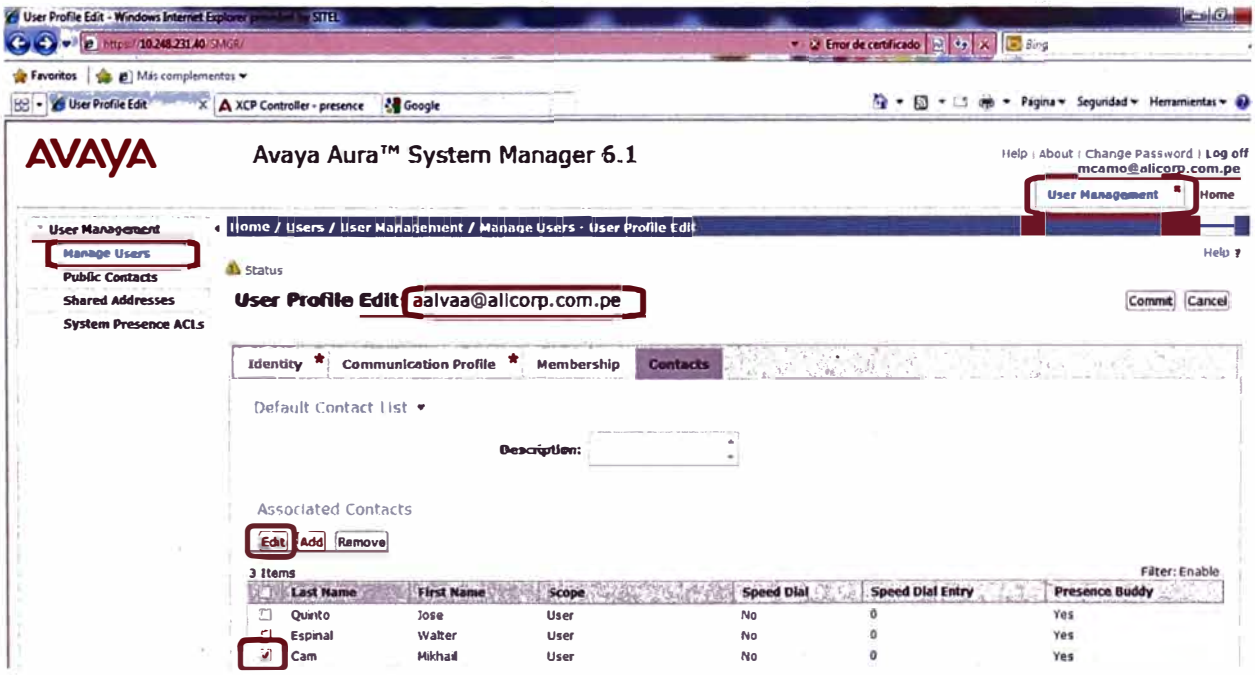


Figura 4.54

Figura 4.55

4.1.5. Puesta en Servicio de Avaya One-X Client Enablement Services

A continuación se describe la puesta en servicio del Avaya One-X Client Enablement Services,

a. Hardware para Avaya One-X Client Enablement Services

Para poner en servicio el Avaya Appication Enablement Services requerimos el siguiente servidor:

- Servidor: IBM x3550 M3, 1U Base
- CPU: 2 x E5507 2.66 Ghz 4-core
- Memoria RAM: 4 x 4GB DDR3 1333Mhz
- Discos Duros: 3 discos duros de 146GB 15K
- Tipo de Raid: 5
- Tarjeta de Red Dual
- Fuente de Poder: 1 x 675 W redundante

b. Instalación de Avaya One-X Client Enablement Services

Lo primero que se debe realizar es instalar el software base System Platform en el servidor x3550 M3, este proceso puede verificarse en el Anexo A. Una vez realizado esto desplegar la imagen de instalador de Avaya One-X Client Enablement Services sobre el System Platform. Para el escenario que estamos describiendo utilizamos la plantilla onexps 6.1.0.0.483 y lo instalaremos de la siguiente manera:

Ingresar al System Platform por consola web a http://ipaddress/ y autenticarse como *admin*.

Ingresar al campo Virtual Machine Management, y luego a Solution Template. Ahí seleccionaremos desde donde se realizará la instalación. En nuestro caso se instaló manera interna luego de subir el template al servidor, escogemos la opción "SP Server".

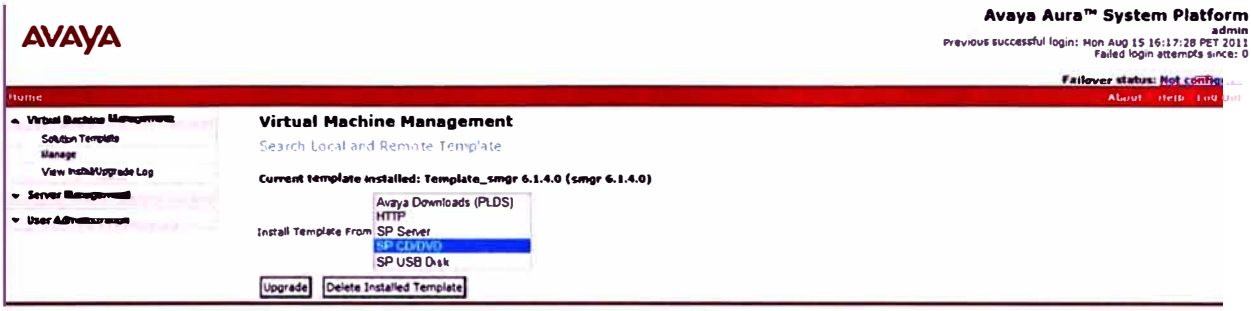
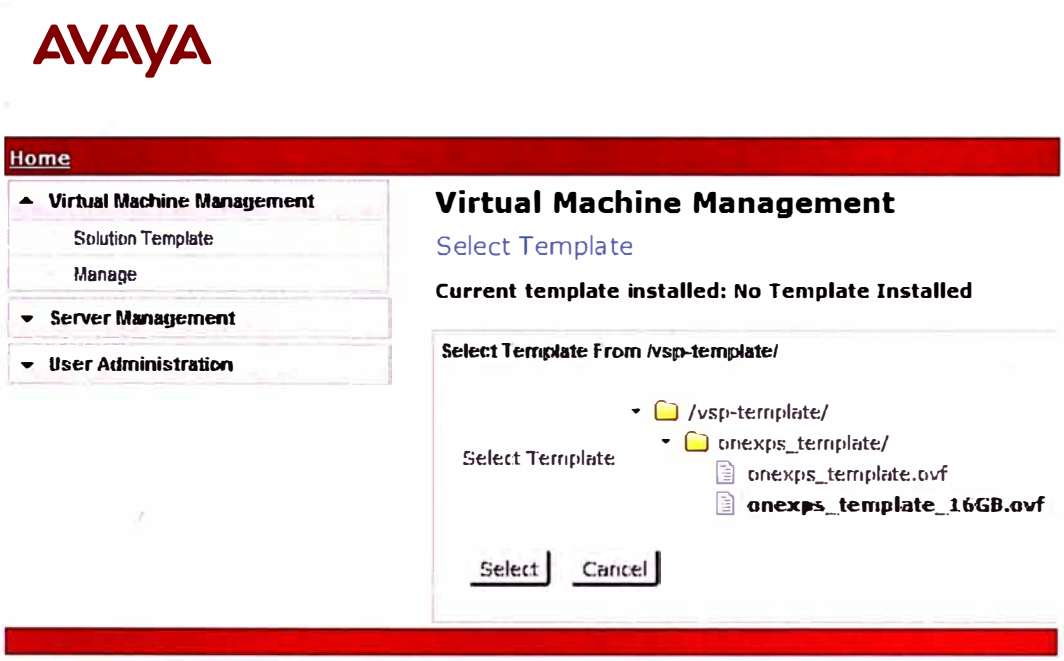


Figura 4.56

Se busca el archivo .ovf de la plantilla y se procede con la instalación.



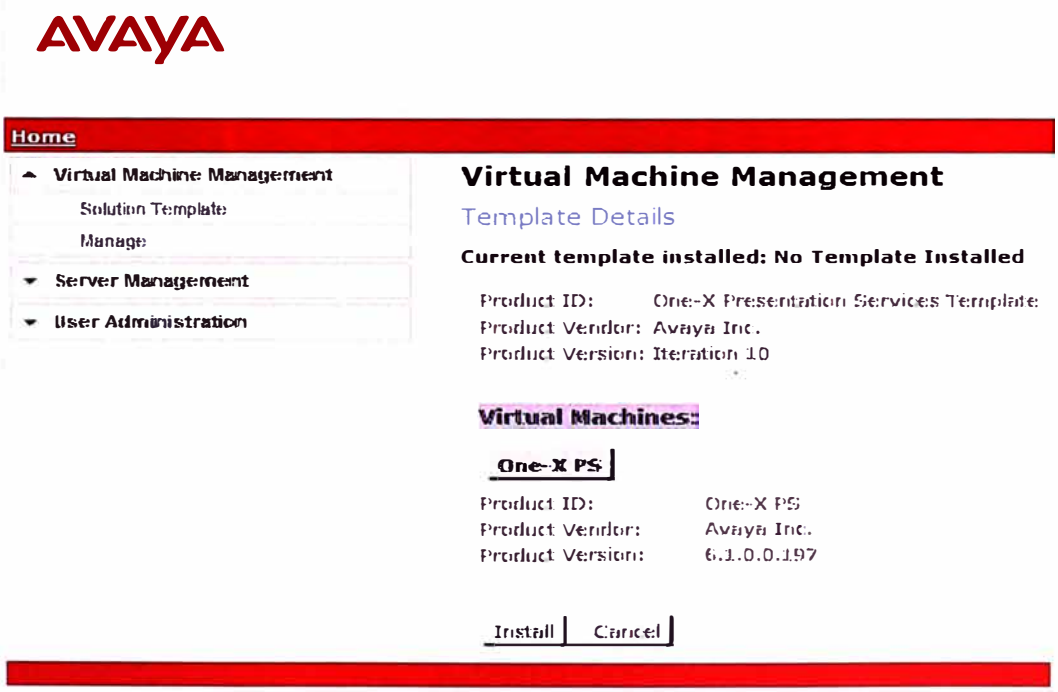


Figura 4.57

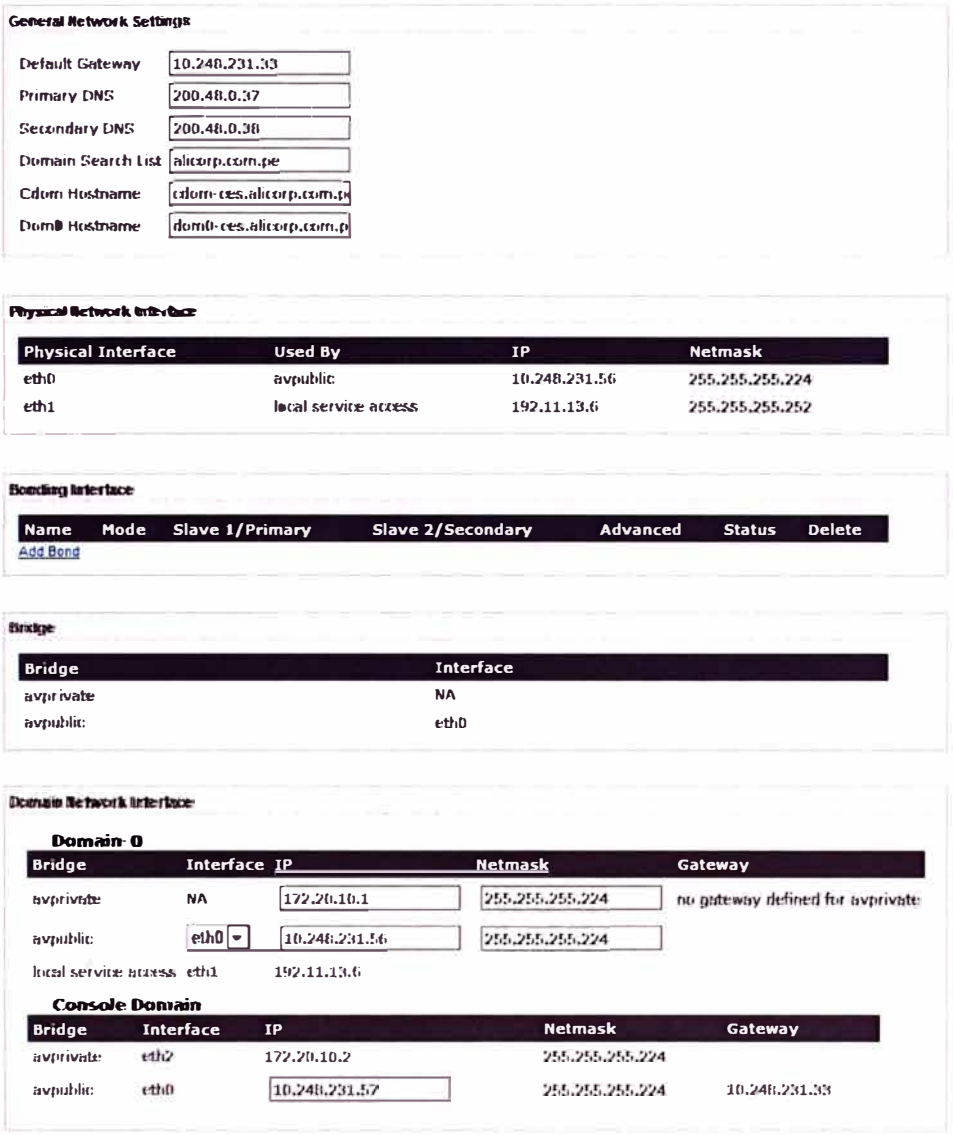


Figura 4.58

Para finalizar la instalación de la plantilla se ejecutará un configurador en el cual se deberán declarar los parámetros de red, los permisos para la base de datos, los permisos para lectura en el Directorio Activo de la empresa, el dominio SIP, el puerto de seguridad para las comunicaciones de los equipos celulares, el password para comunicarse con el SMGR

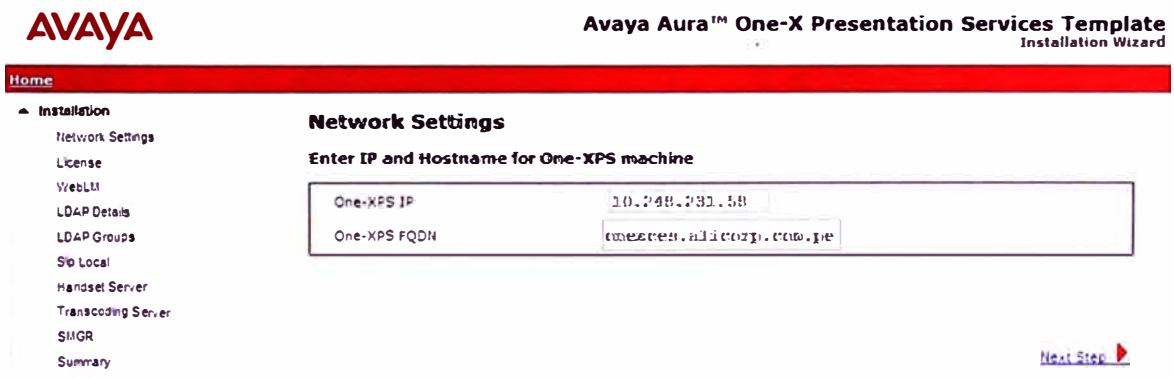


Figura 4.59

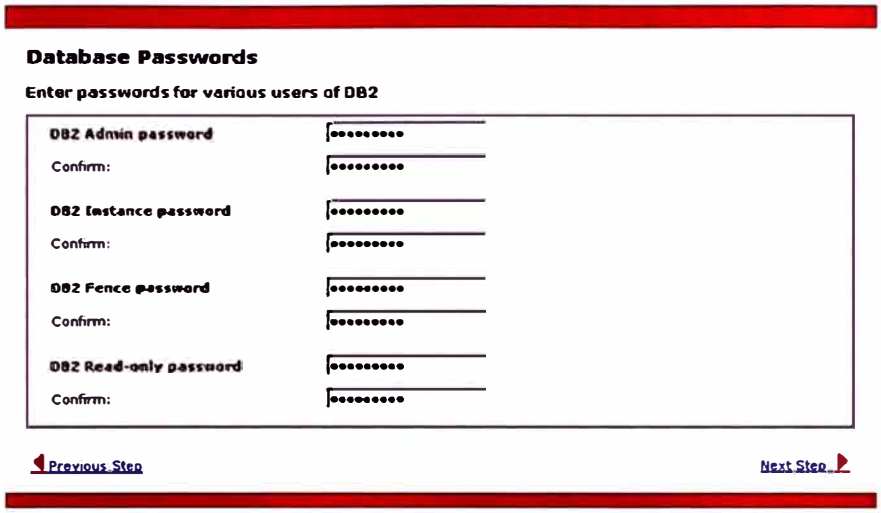


Figura 4.60

Figura 4.61

Figura 4.62

Figura 4.63

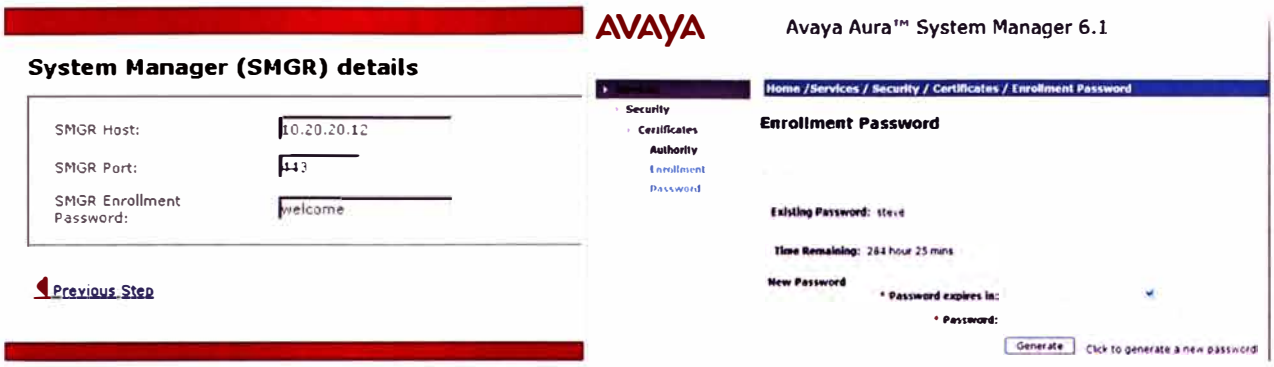


Figura 4.64

El proceso de instalación puede verse dentro de Virtual Machine Management, en View Install/Upgrade Log.

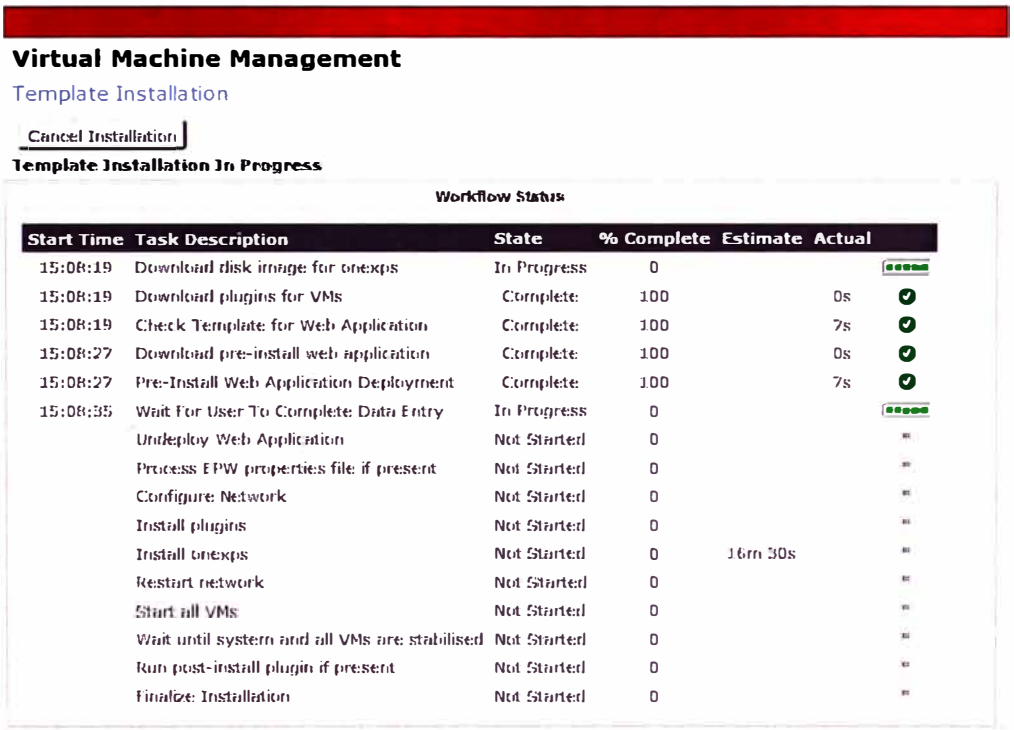


Figura 4.65

Luego se verifica el estado de la aplicación instalada. Dentro de Virtual Machine Management se ingresa a Manage y se elige la aplicación "one-X CES

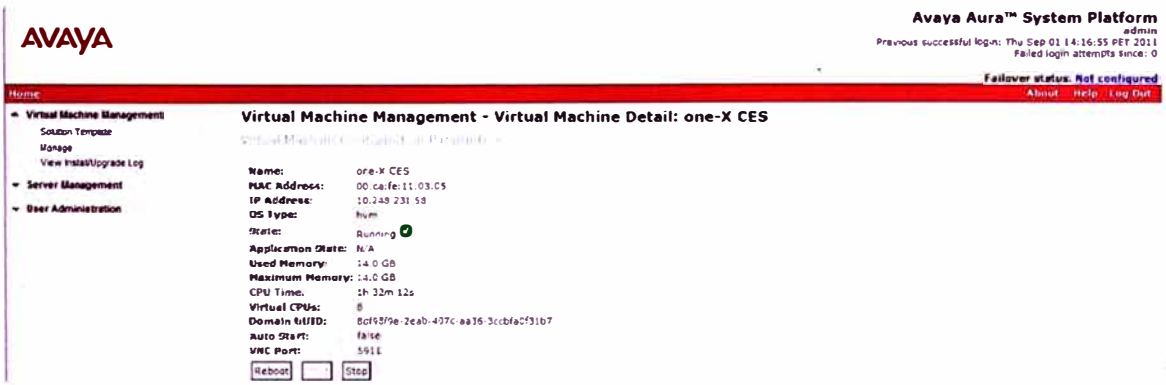


Figura 4.66

Verificamos el ingreso correcto al Avaya One-X Client Enablement Services ingresando al explorador el siguiente URL https://ipadress:9443/admin/logon.jsp colocando la IP que se haya configurado y luego comprobar el usuario y password configurados.

Figura 4.67

c. Inicialización de Avaya One-X Client Enablement Services

Ingresamos a la consola web de Avaya One-X Client Enablement Services y veremos la pantalla principal, ingresamos a *Servers* para configurar los servidores con los que deberá comunicar.

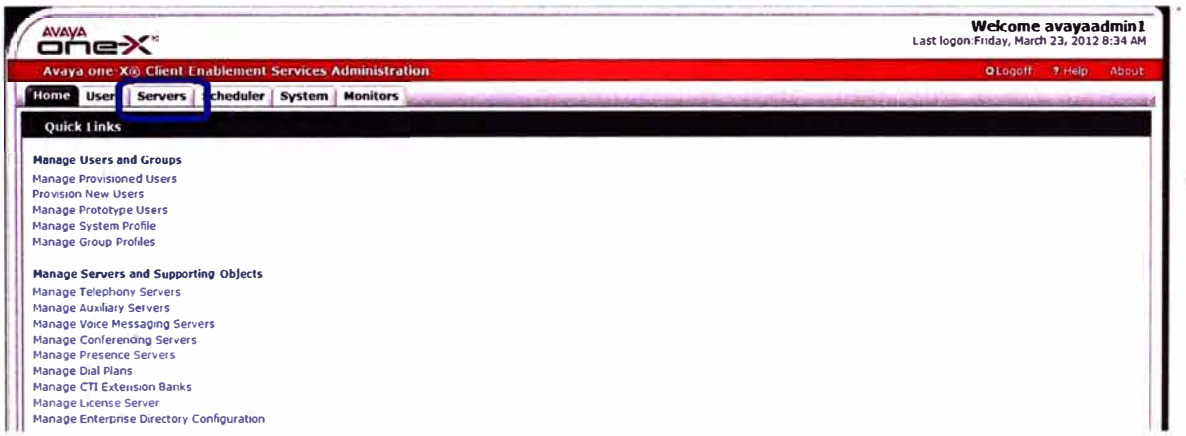


Figura 4.68

El primero servidor en declarar es el Avaya Communication Manager, cuyos parámetros son declarados en el apartado de *Telephony*.

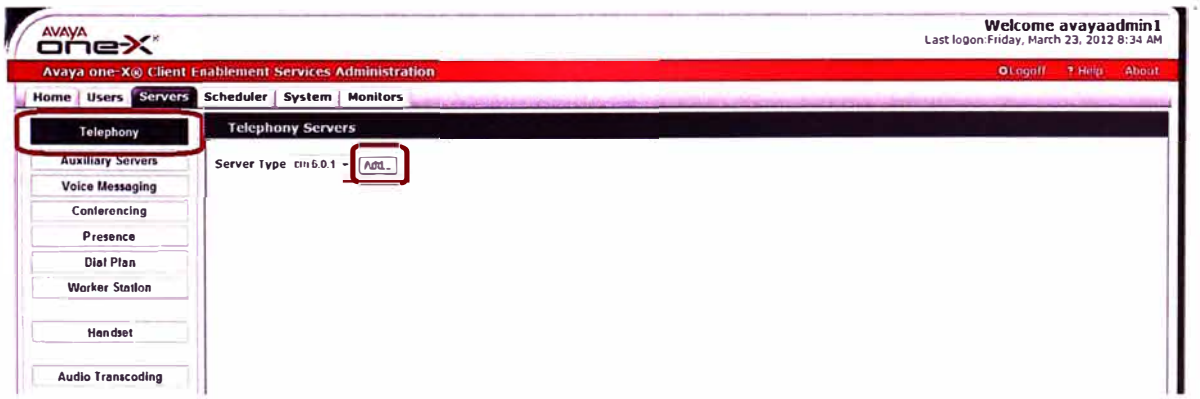


Figura 4.69

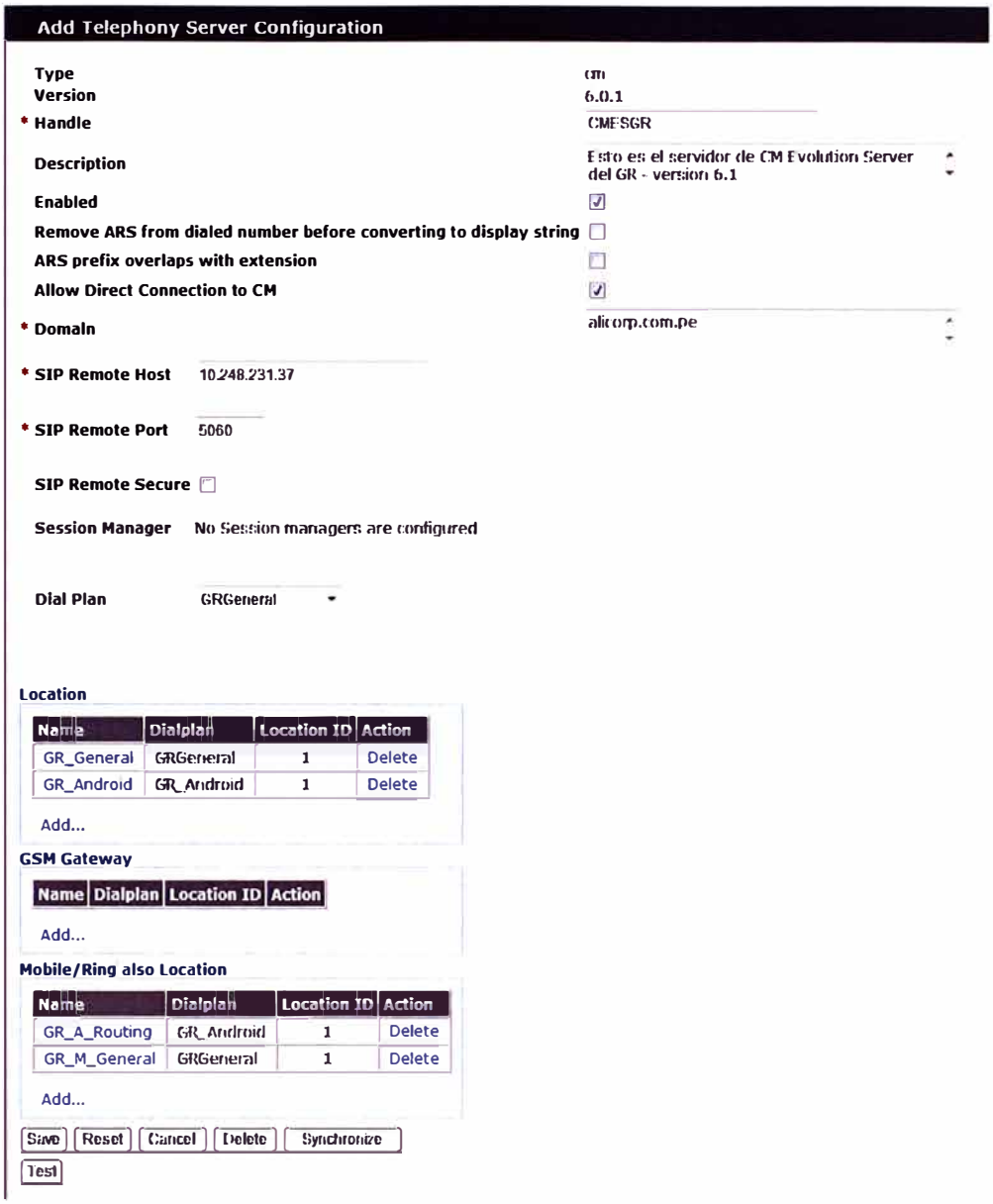


Figura 4.70

Luego se declara el Avaya Communication Manager Messaging para el acceso a las casillas de voz de los usuarios, los parámetros son declarados en el apartado de *Voice Messaging*.

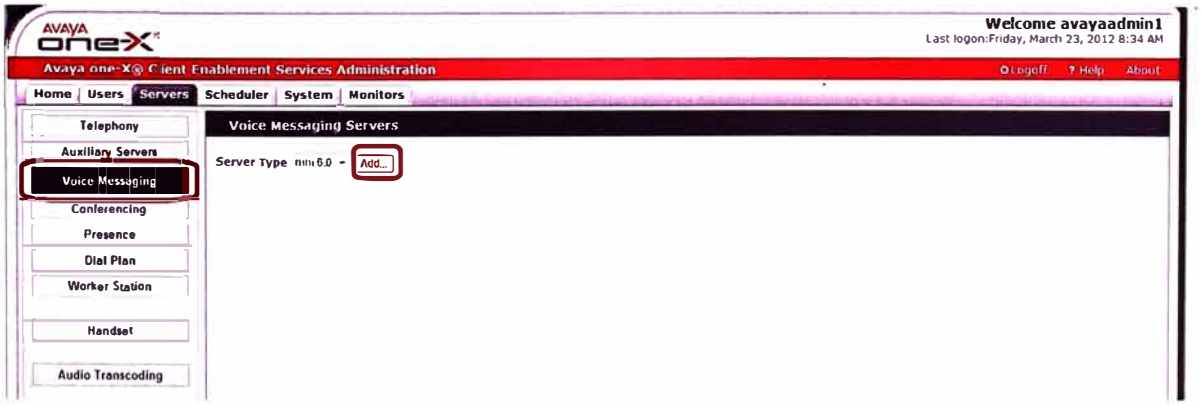


Figura 4.71

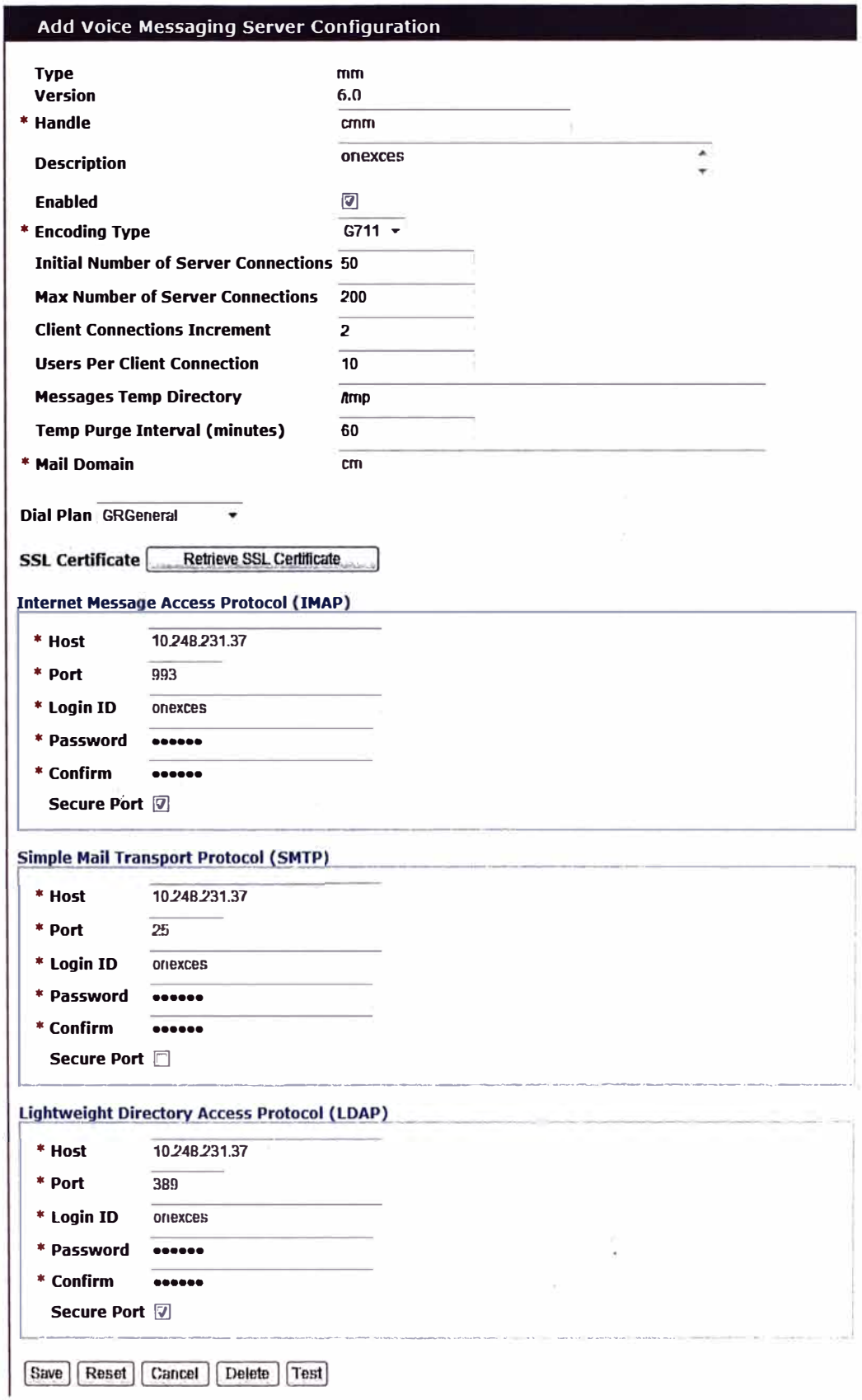


Figura 4.72

Luego se declara el Avaya Presence Services para el acceso al estado de presencia de cada usuario, los parámetros son declarados en el apartado de *Presence*, siempre dentro de la categoría *Servers*.

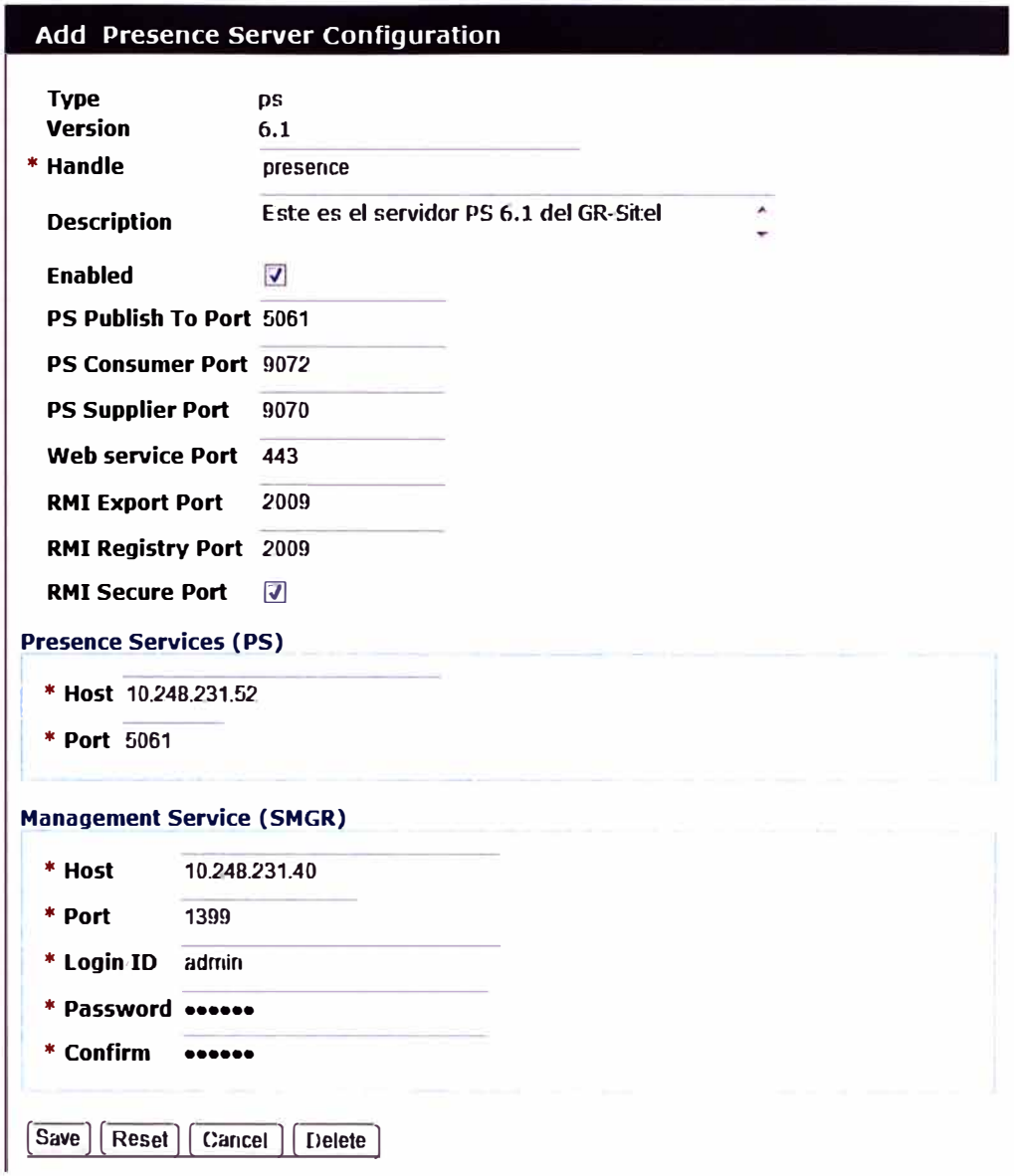


Figura 4.73

Se define luego el Plan de Marcación que deberá seguir el Avaya One-X Client Enablement Services para sus llamadas, esto dentro del apartado *Dial Plan*.

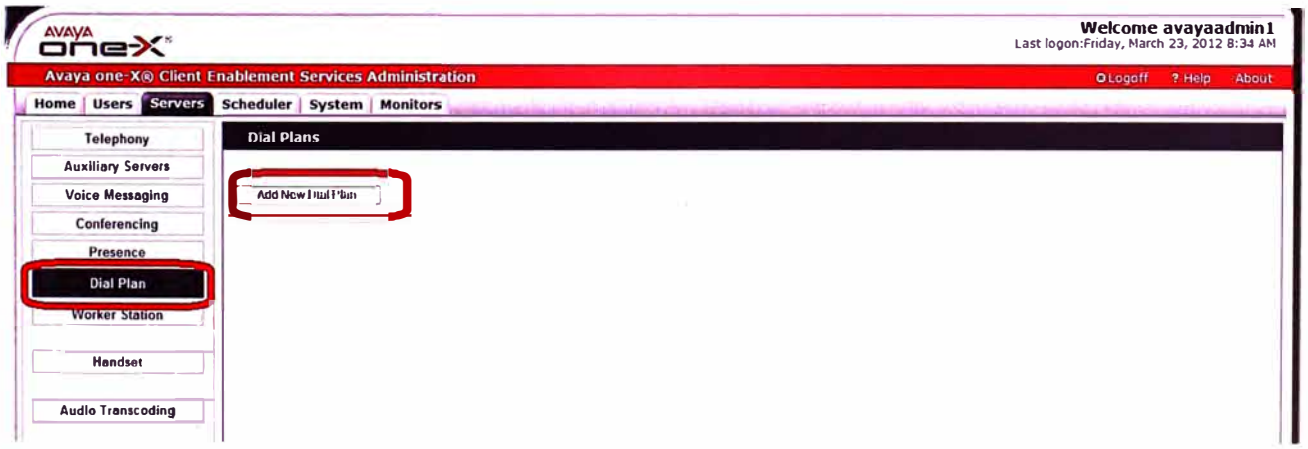


Figura 4.74

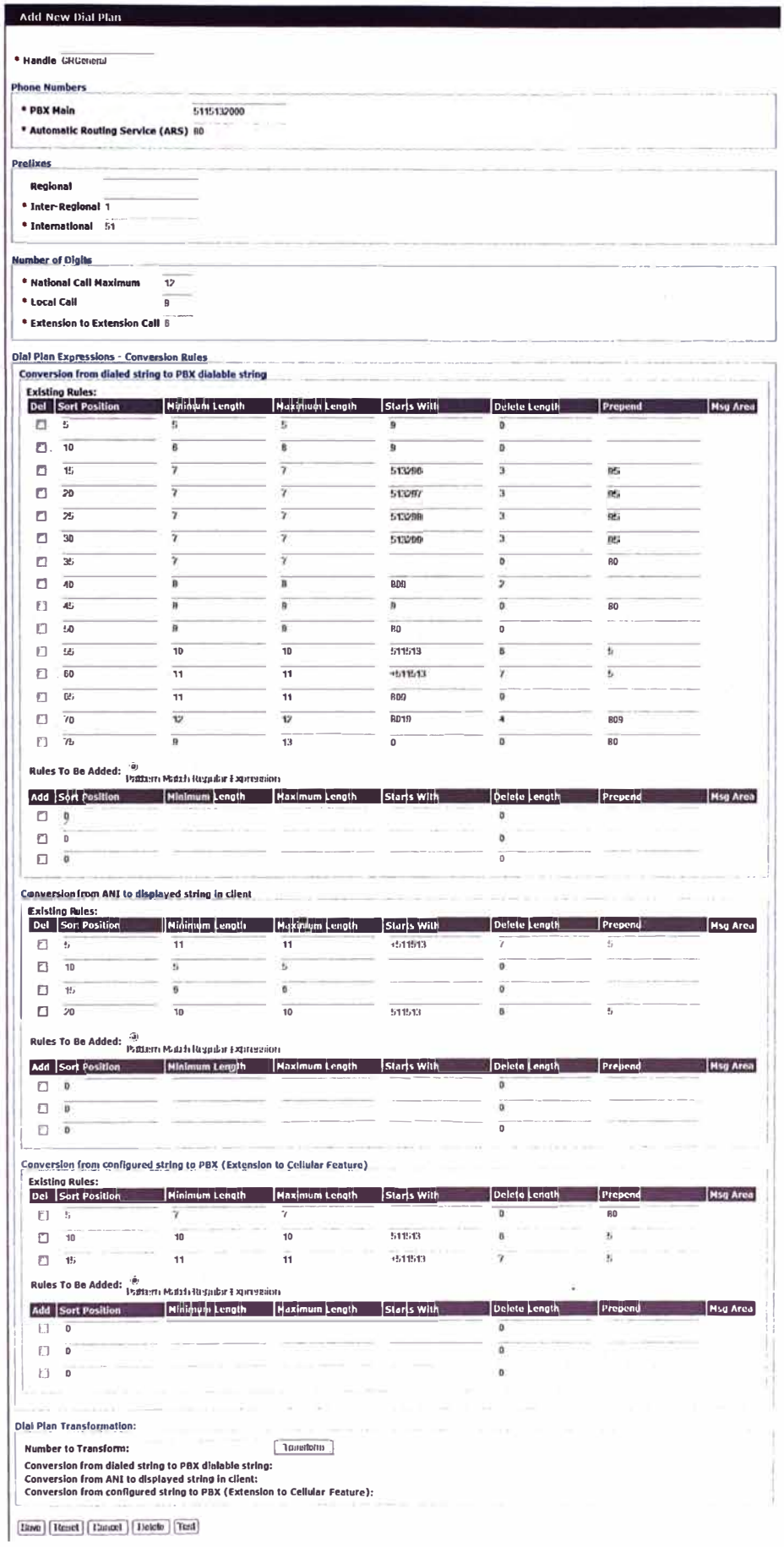

Add New Dial Plan
* Handle GRGeneral
Phone Numbers
* PBX Main 5115132000
* Automatic Routing Service (ARS) 80
Prefixes
Regional
* Inter-Regional 1
* International 51
Number of Digits
* National Call Maximum 12
* Local Call 8
* Extension to Extension Call 8
Dial Plan Expressions - Conversion Rules
Conversion from dialed string to PBX dialable string
Existing Rules:
Del | Sort Position | Minimum Length | Maximum Length | Starts With | Delete Length | Prepend | Msg Area
Rules To Be Added:
Pattern Match Regular Expression
Add | Sort Position | Minimum Length | Maximum Length | Starts With | Delete Length | Prepend | Msg Area
Conversion from ANI to displayed string in client
Existing Rules:
Del | Sort Position | Minimum Length | Maximum Length | Starts With | Delete Length | Prepend | Msg Area
Rules To Be Added:
Pattern Match Regular Expression
Add | Sort Position | Minimum Length | Maximum Length | Starts With | Delete Length | Prepend | Msg Area
Conversion from configured string to PBX (Extension to Cellular Feature)
Existing Rules:
Del | Sort Position | Minimum Length | Maximum Length | Starts With | Delete Length | Prepend | Msg Area
Rules To Be Added:
Pattern Match Regular Expression
Add | Sort Position | Minimum Length | Maximum Length | Starts With | Delete Length | Prepend | Msg Area
Dial Plan Transformation:
Number to Transform:
Transform
Conversion from dialed string to PBX dialable string:
Conversion from ANI to displayed string in client:
Conversion from configured string to PBX (Extension to Cellular Feature):
Save
Reset
Cancel
Delete
Test

Figura 4.75

Luego dentro de la categoría *System*, en el apartado *Enterprise Directory* configuramos los parámetros del Directorio Activo al cual se harán consultas por los perfiles de los usuarios.

Figura 4.76

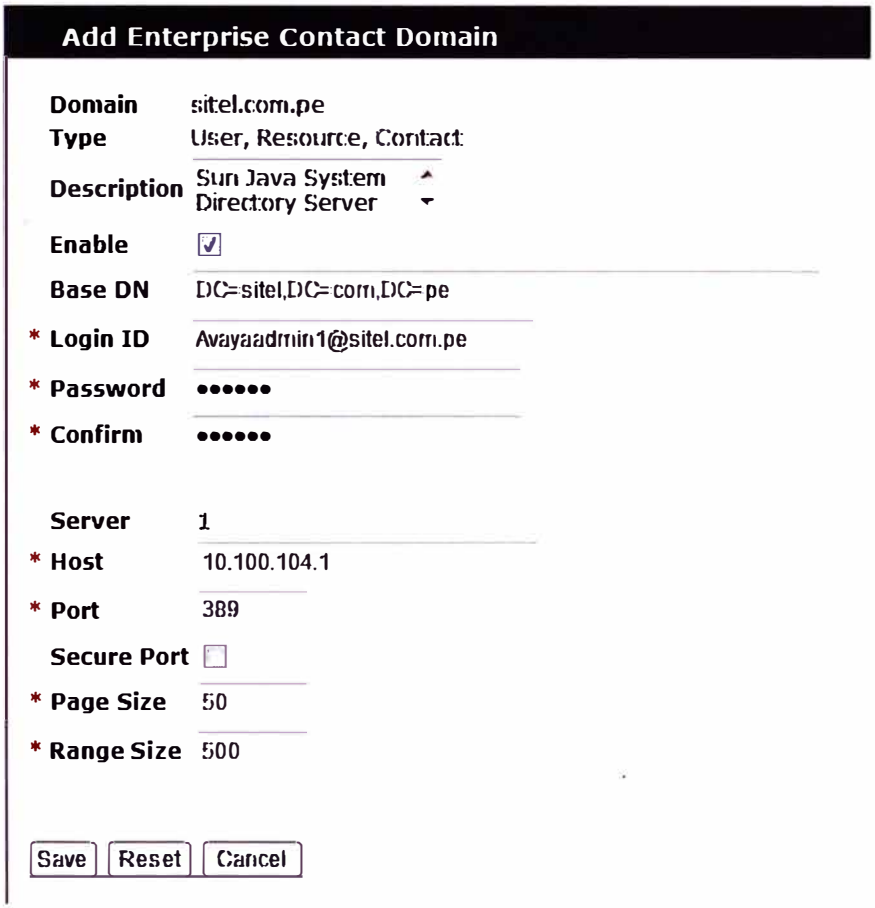


Figura 4.77

Luego declaramos el dominio SIP al que pertenece el servidor, su dirección IP y el puerto con el que se comunicará vía SIP. Esto dentro de la categoría *System* y en el apartado *SIP Local*.

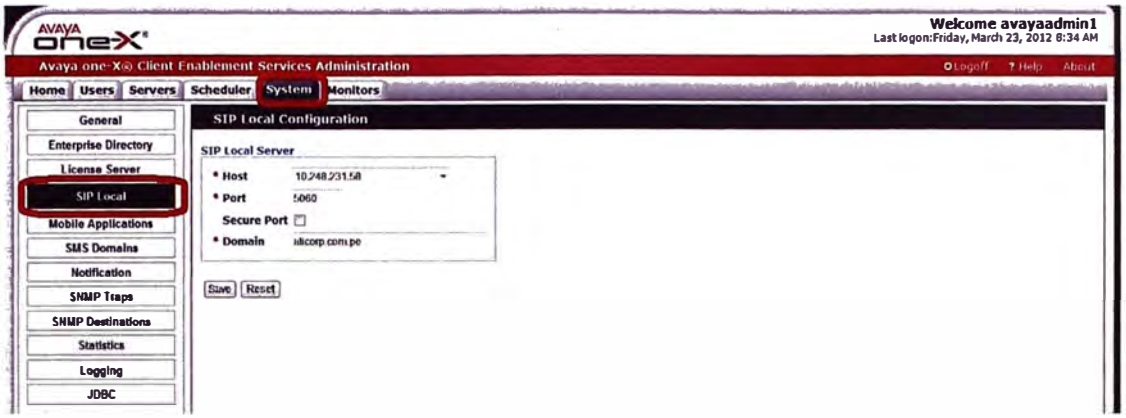


Figura 4.78

Finalmente, para agregar a los usuarios del servicio debemos ir a la categoría *Users* e ingresar al apartado *Unprovisioned Users*, colocaremos la cuenta de red del usuario deseado y damos clic al botón *Provision*…

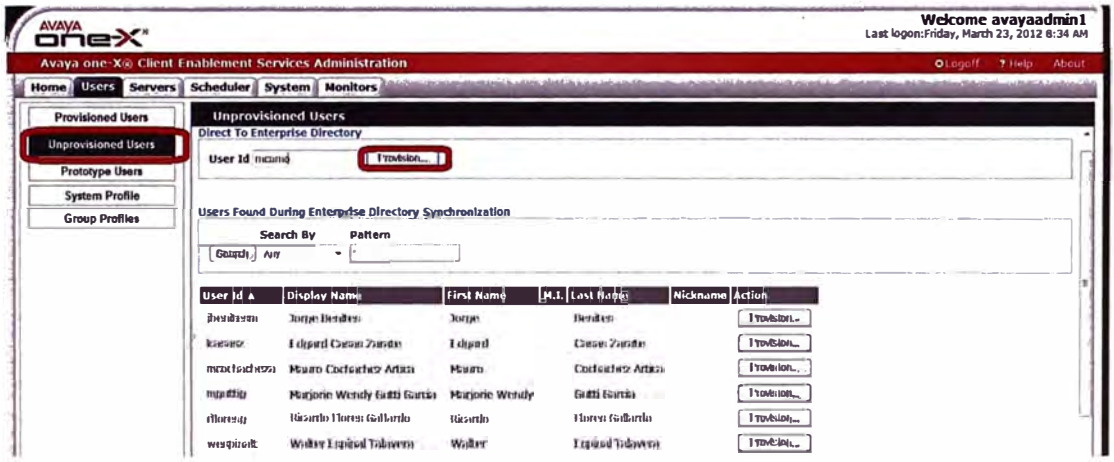


Figura 4.79

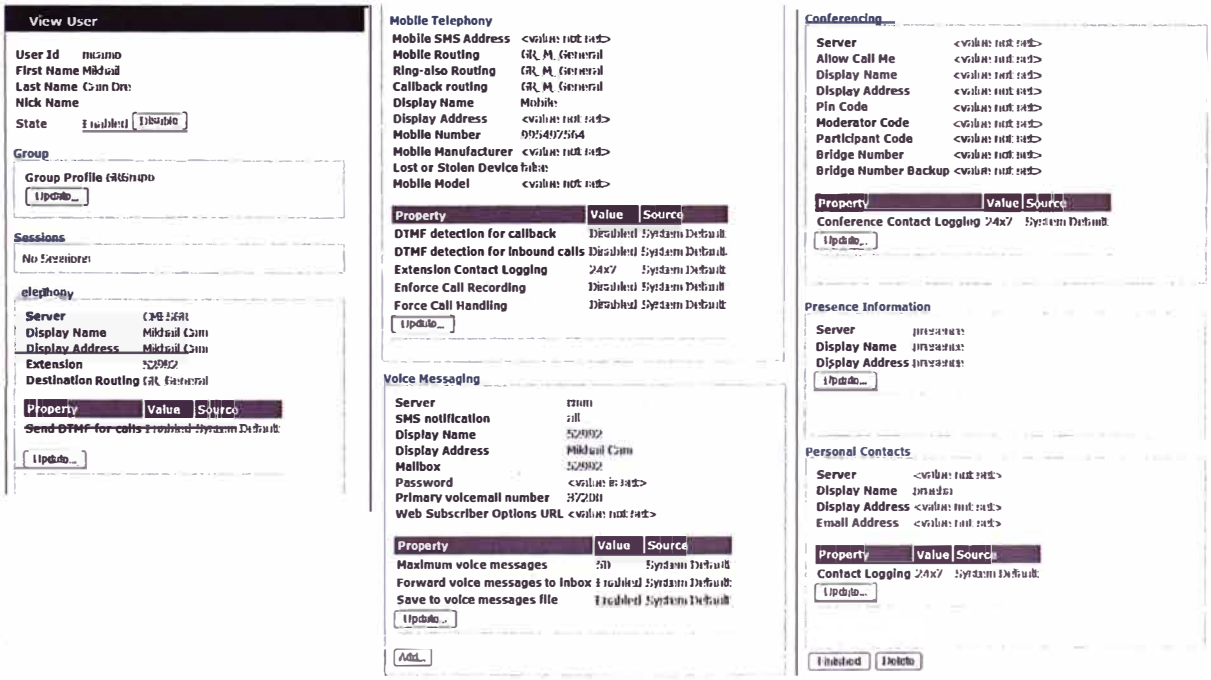


Figura 4.80

4.1.6. Puesta en Servicio de Avaya One-X Deskphone 9600 Series

Para poner en servicio los Avaya One-X Deskphone sólo requerimos una conexión a la red de datos local del usuario, de preferencia Power Over Ethernet (PoE) o en su defecto conectaríamos el teléfono junto con la fuente de poder que se conectaría a una toma eléctrica. Ingresamos a la configuración de red del equipo y llenamos los parámetros de dirección IP, máscara de red, Gateway, Servidor HTTP y HTTPS (esto para bajar las actualizaciones de firmware), SIP Proxy (dirección de Avaya Session Manager) y en el caso se requiera se coloca el ID de la VLAN correspondiente.

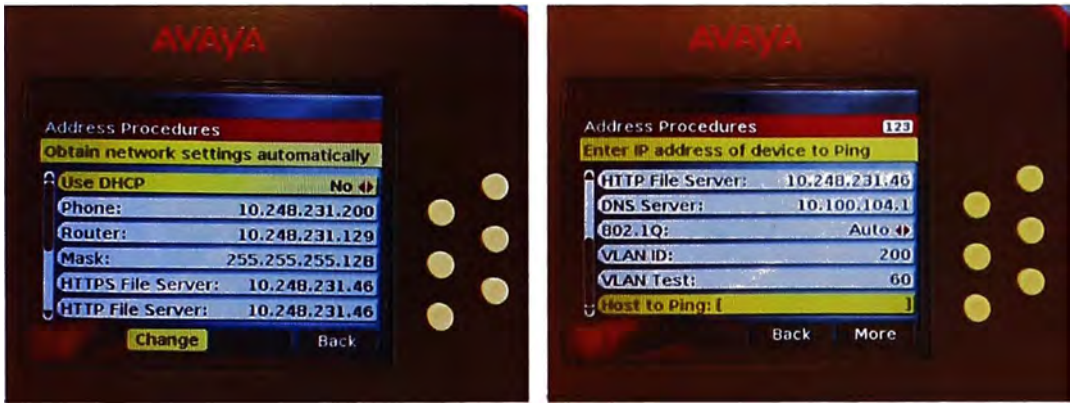


Figura 4.81 Configuración de parametros IP de un Avaya One-X Deskphone

Luego de configurar los parámetros el equipo se reinicia y terminado este proceso nos muestra la ventana de logueo y estaría listo para ser usado.

Figura 4.82 Ventana de logueo de un Avaya One-X Deskphone

4.1.7. Puesta en Servicio de Avaya One-X Communicator

Lo primero que se verifica es la correcta instalación y configuración del aplicativo, cuyas recomendaciones para la PC del usuario son:

- Procesador Intel Pentium 1.2 GHz (mínimo)
- 1.5 GB de memoria RAM (más para Windows Vista y Windows 7)
- 1.5 GB de espacio de disco duro libre (mínimo)
- Monitor de alta resolución (1024 x 768)
- Tarjeta de red

- Head Set

  Adicionalmente se requiere tener el siguiente software instalado en la PC:

- Microsoft .NET Framework 4
- Microsoft Visual C++ 2005 SP1
- Microsoft DirectX

Figura 4.83 Confirmación de instalación de One-X Communicator

Luego de haber instalado el One-X Communicator se procede a configurarlo indicando la dirección IP de Avaya Session Manager y Avaya Presence Services, el nombre de dominio, propiedades y reglas de marcación y la integración con el Directorio Activo de la empresa.

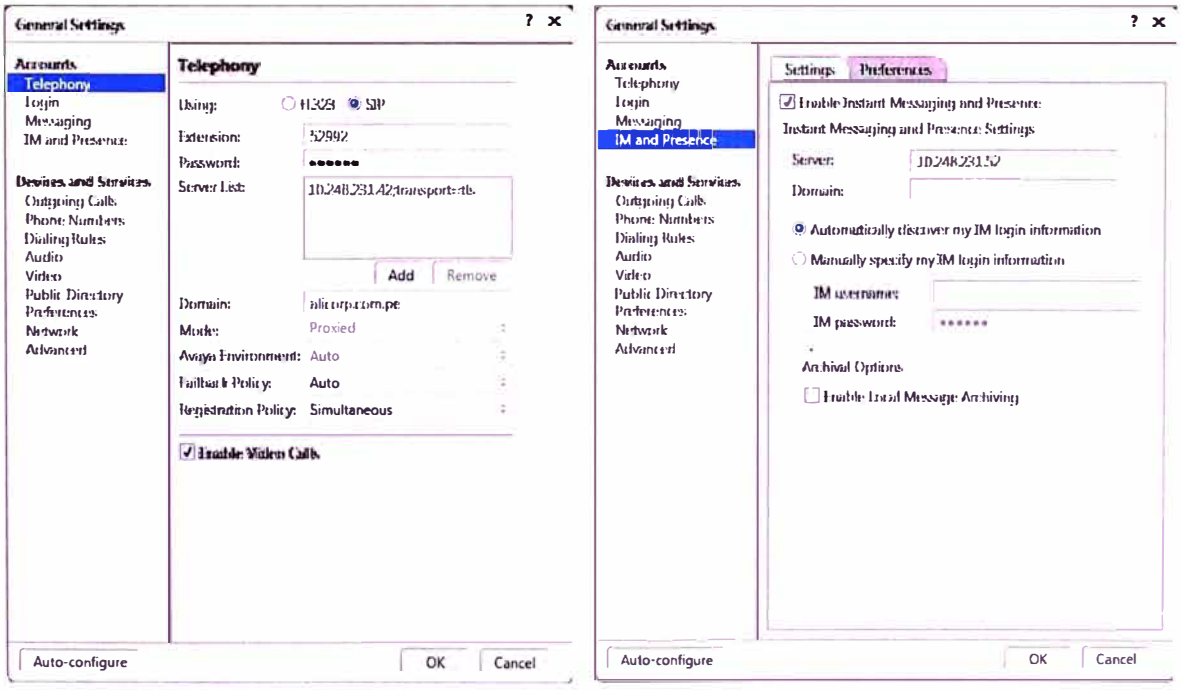


Figura 4.84 Ventanas de configuración de One-X Communicator

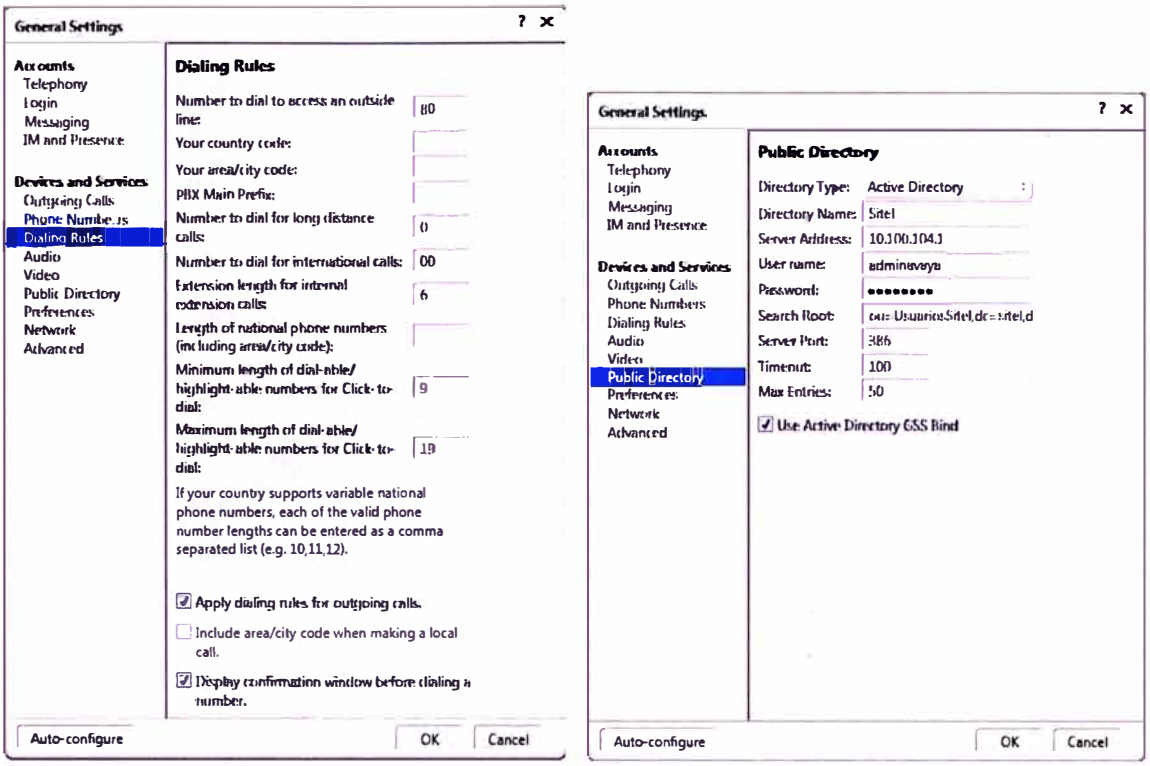


Figura 4.85 Ventanas de configuración de One-X Communicator

Luego de realizar estas configuraciones el aplicativo se reinicia y nos presenta la ventana de logueo de usuario SIP y está listo para ser utilizado.

Figura 4.86 Ventana de logueo de usuario de One-X Communicator

4.1.8. Puesta en Servicio de Avaya One-X Mobile

Avaya One-X Mobile es un software cliente que se encuentra disponible para equipos iPhone, Blackberry y equipos con sistema Android. Los equipos que al momento de realizar este Informe soportan Avaya One-X Mobile son:

- iPhone (Apple): 3G, 3GS, 4 y 4S
- Blackberry (RIM): Bold 9650, Bold 9700, Curve 8520, Curve 8900, Curve 9300, Perl 9105, Storm 2 (9550)
- Android: Moto Droid 2, HTC Mytouch 4G, Samsung Galaxy, Dell Streak

Para el caso de Blackberry se tiene que instalar el aplicativo conectando el equipo móvil a una PC que tenga instalado el software Blackberry Desktop, el cual nos permitirá ingresar e instalar el Avaya One-X Mobile en el equipo Blackberry.

En el caso de equipos Android el aplicativo se descarga desde el Android Market, al cual podemos acceder desde el equipo móvil y descargarlo para su instalación directa.

En este presente Informe tomaremos como ejemplo la puesta en servicio del Avaya One-X Mobile en un equipo iPhone con el cual haremos las verificaciones posteriores del servicio. Para dicho caso el aplicativo se debe descargar desde el App Store, usando la opción de búsqueda.

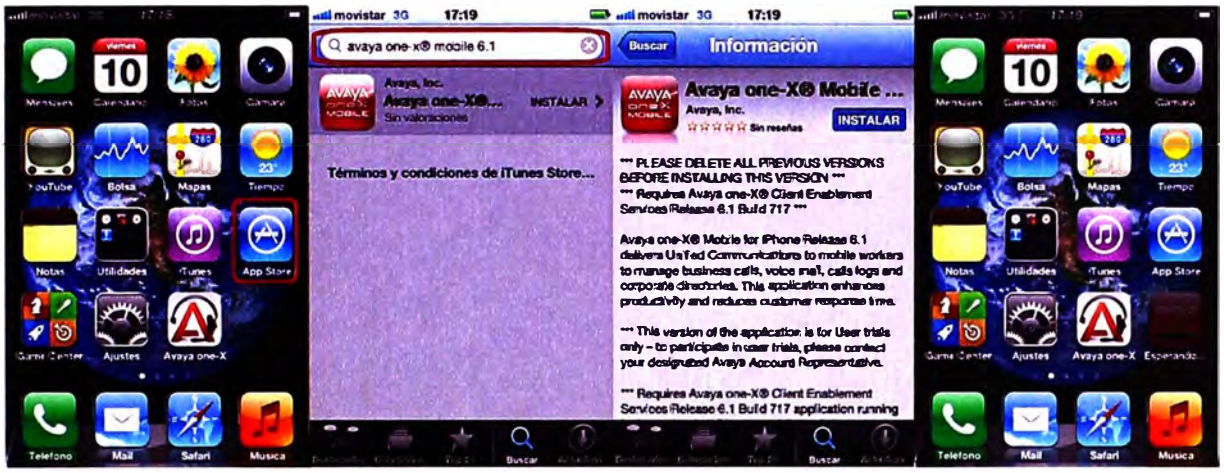


Figura 4.87 Instalación de One-X Mobile en iPhone

Luego de descargar el aplicativo este se instala automáticamente en el equipo. Ingresamos al ícono respectivo para iniciar el aplicativo por primera vez y colocamos los datos de usuario necesarios para que el aplicativo se conecte al servidor Avaya One-X Client Enablement Services (usuario, password, URL del servidor, puerto y seguridad).

Figura 4.88 Configuración de One-X Mobile en iPhone

4.1.9. Puesta en Servicio de Avaya Desktop Video Device

Encendemos el equipo y lo primero que debemos hacer es configurar los parámetros IP para que pueda ser conectado a la red corporativa. Se verá un icono de red desconectada en la esquina superior derecha de la pantalla, lo tocamos y tendremos opción a colocar los parámetros como dirección IP, máscara de red, dirección de Gateway, VLAN y DNS's del equipo.

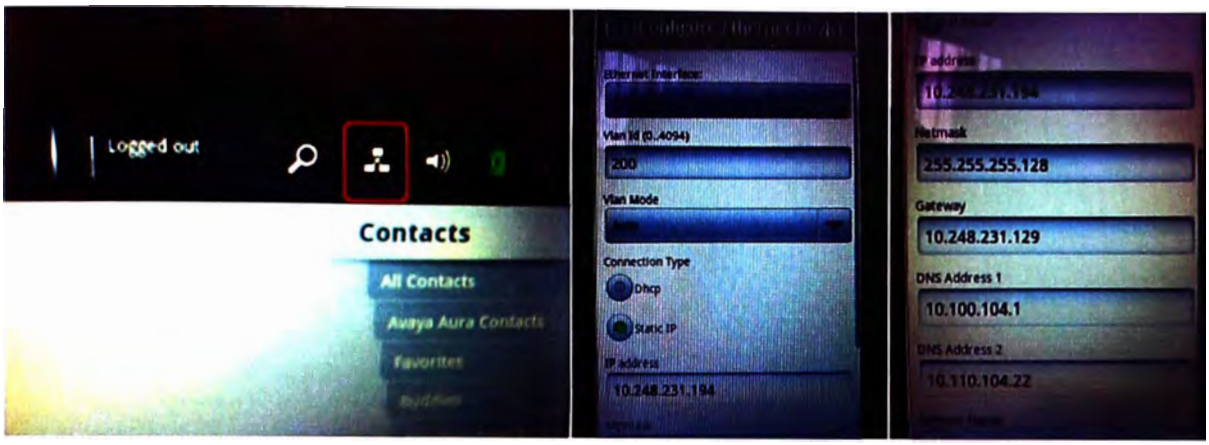


Figura 4.89 Parámetros de red de Avaya Desktop Video Device

Una vez conectado a la Red del Grupo procedemos a configurarlo buscando el ícono *Opciones* en el menú izquierdo, dentro de lo cual entramos a *Opciones de Administrador*, la primera opción que encontramos es la *Dirección del File Server*.

Figura 4.90 Menú *Opciones de Administrador* Avaya Desktop Video Device

Ingresamos la dirección del Utility Server, que actúa como File Server para que los equipos descarguen alguna actualización que se encuentre disponible cada vez que sean encendidos.

Figura 4.91 Seteo de *Dirección de File Server* en Avaya Desktop Video Device

Luego dentro *Opciones de Administrador* ingresamos a la categoría *Opciones SIP* para configurar todos los parámetros SIP necesarios para el equipo.

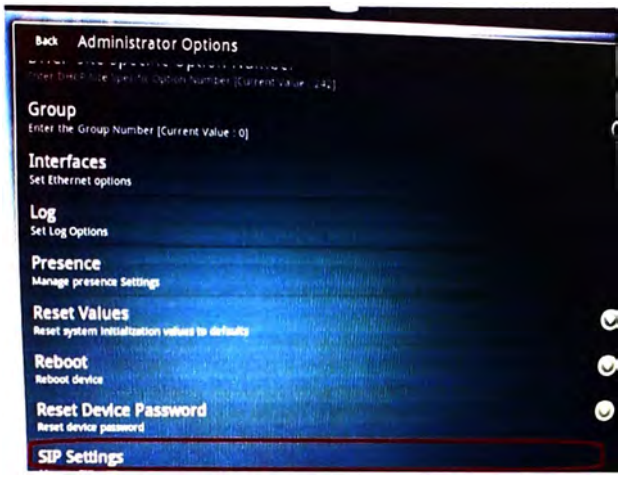


Figura 4.92 Menú *Opciones de Administrador* en Avaya Desktop Video Device

Dentro de las *Opciones SIP* ingresamos a la primera opción *Opciones Globales SIP*, dentro de esto se coloca el modo Proxy, el dominio SIP, la política de registro y la política de Failback.

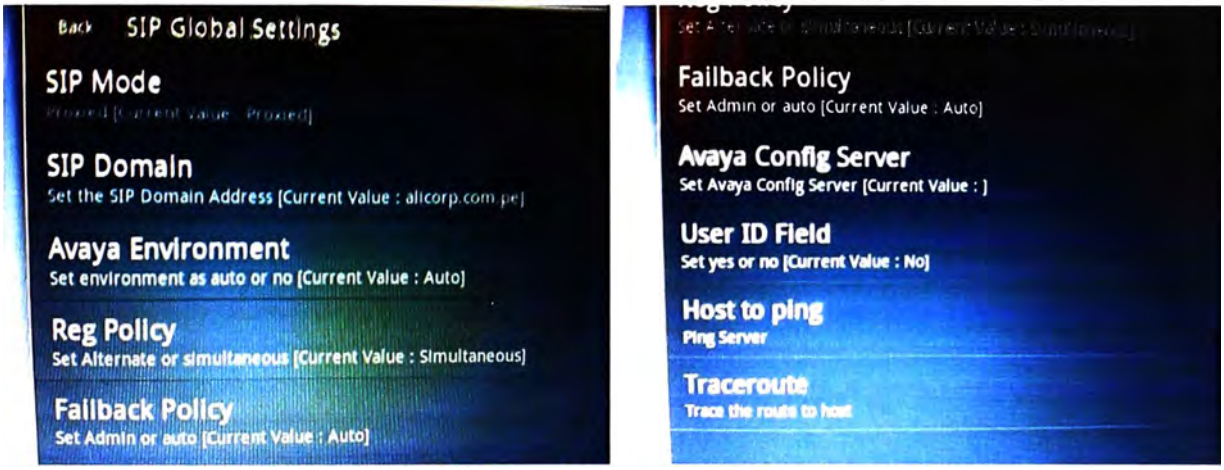


Figura 4.93 Seteo de *Opciones Globales SIP* en Avaya Desktop Video Device

Luego retornamos a *Opciones SIP* e ingresamos a la segunda opción *Opciones Proxy SIP*, dentro de lo cual agregaremos un nuevo SIP Proxy Server que es Avaya Session Manager y su puerto respectivo.

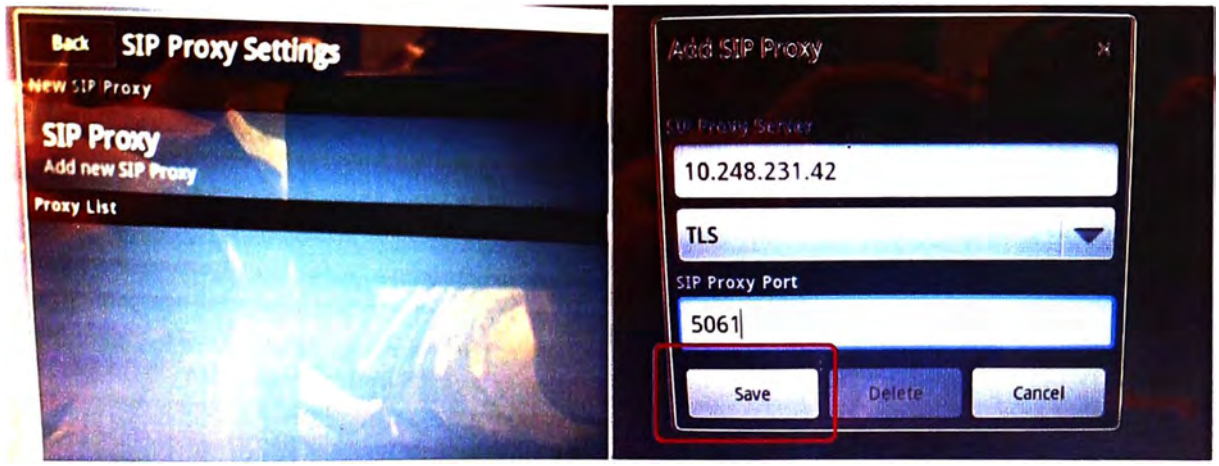


Figura 4.94 Seteo de *Opciones Proxy SIP* en Avaya Desktop Video Device

Luego tocamos el ícono de correo en la esquina superior izquierda para configurar una cuenta de correo Exchange, colocamos los datos de usuario, password, dirección IP del servidor

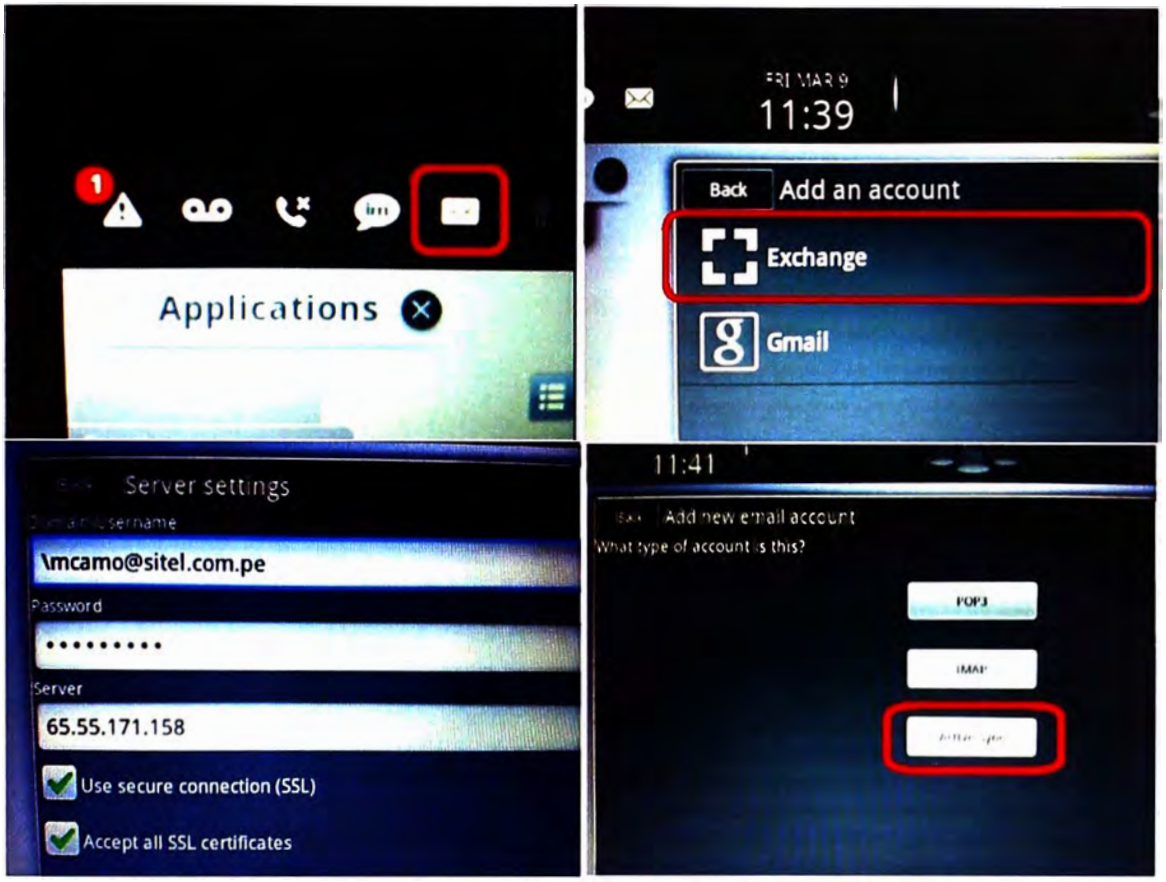


Figura 4.95 Configuración de correo Exchange en Avaya Desktop Video Device

Una vez que se validan las credenciales de la cuenta se configura las opciones sincronización aparte del correo como la libreta de contactos o la agenda de la cuenta corporativa, con lo que terminaría la configuración de correo en el equipo.

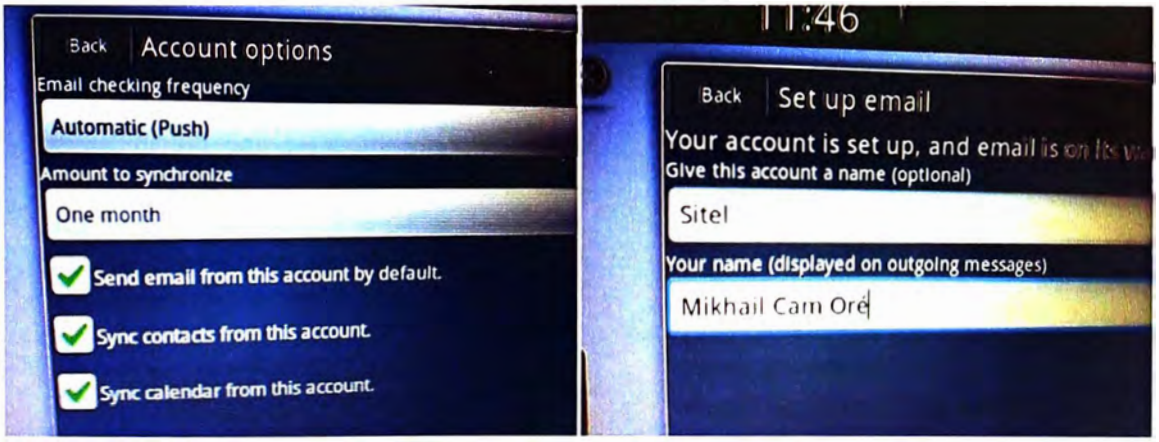


Figura 4.96 Opciones de sincronización de correo corporativo en Avaya Desktop Video Device

Finalmente si el usuario lo desea puede sincronizar su cuenta de Facebook en el Avaya Desktop Video Device

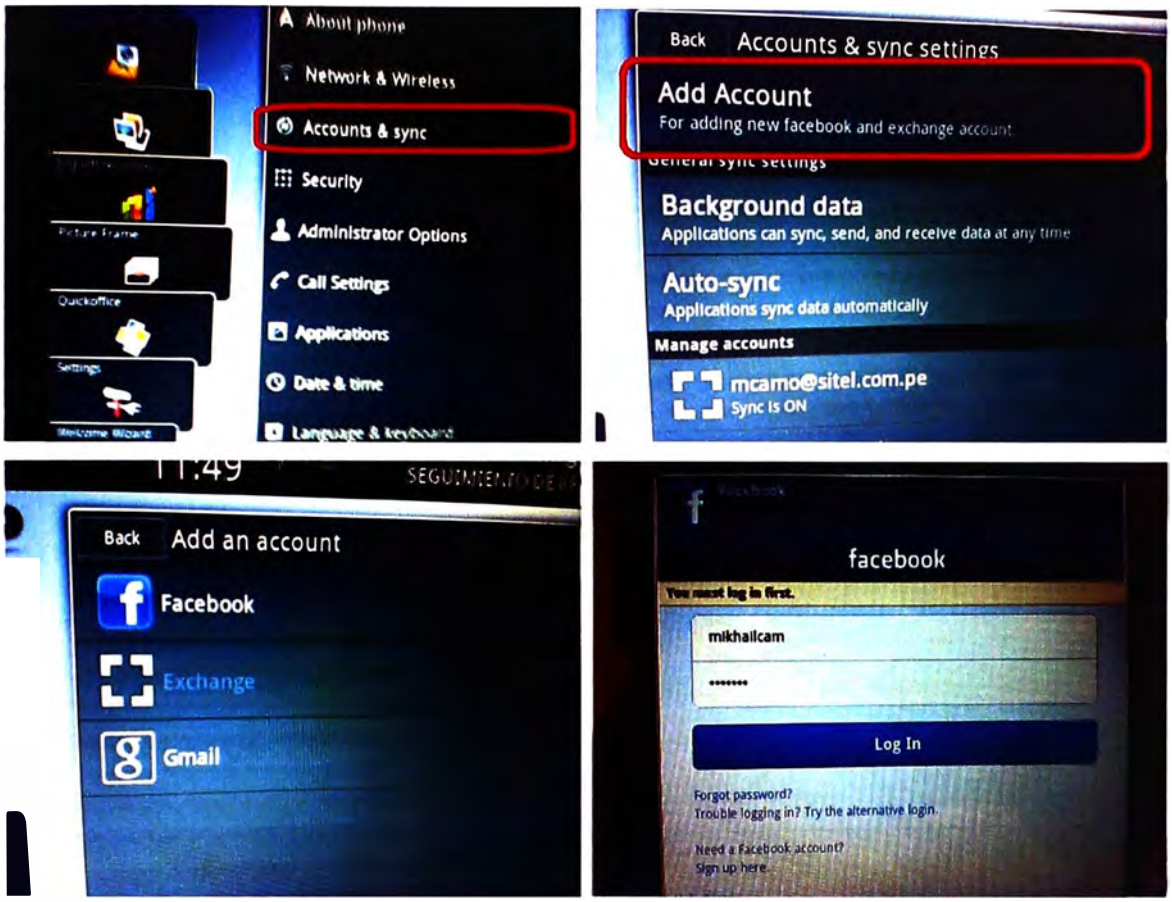


Figura 4.97 Activación de cuenta de Facebook en Avaya Desktop Video Device

4.1.10. Puesta en Servicio de Avaya Flare Communicator

Tal como se mencionó anteriormente, se disponen de 2 versiones para este aplicativo. A continuación describimos las configuraciones para ambos casos:

a. Puesta en Servicio de Avaya Flare Communicator para iPad

El único requisito de hardware para este aplicativo es que el usuario cuente con un iPad2. El usuario ingresará entonces al App Store para descargar el aplicativo de forma gratuita y tocando el botón INSTALAR según se muestra en la figura.

Figura 4.98 Instalación de Flare Communicator para iPad

Luego de terminada la instalación ingresamos al aplicativo por primera vez tocando el icono respectivo del aplicativo y veremos el Contrato de Licencia de Usuario Final al cua sólo le damos “Aceptar” y nos permitirá configurar el aplicativo.

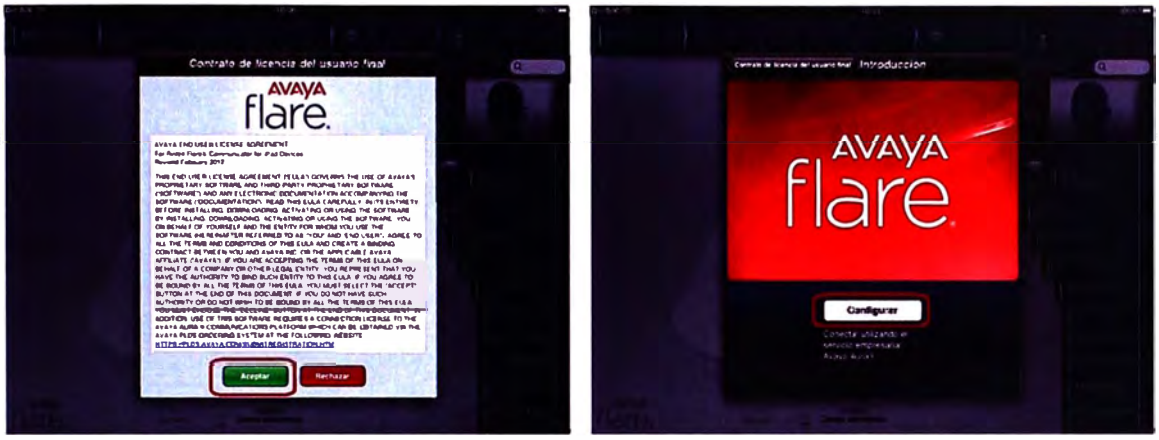


Figura 4.99 Contrato de Licencia de Usuario de Flare Communicator para iPad

Al ingresar a la configuración del aplicativo colocaremos los datos de Avaya Session Manager, dominio SIP, Avaya Presence Services, integración con el Directorio activo de la empresa del usuario y las reglas de marcado respectivas.

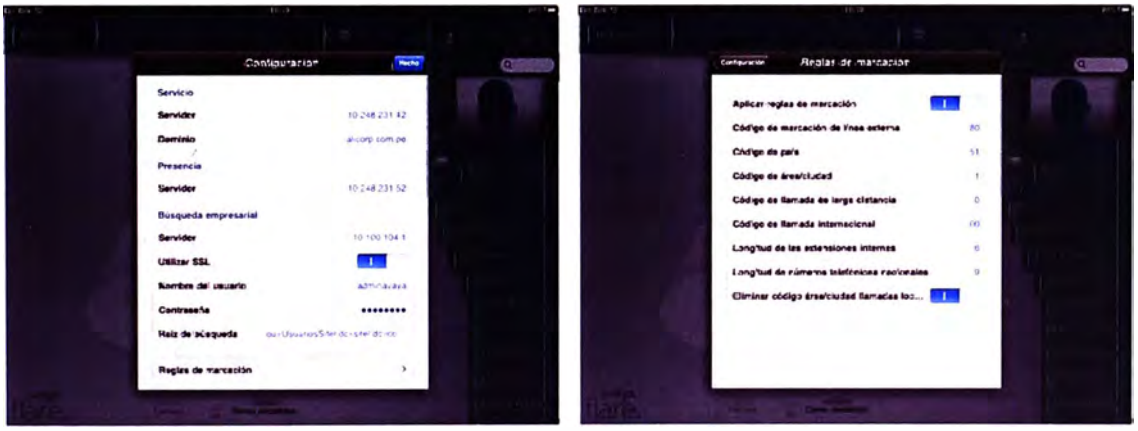


Figura 4.100 Configuración de Flare Communicator para iPad

Terminado esto el aplicativo está listo para ser usado y nos lleva a la ventana principal para que el usuario ingrese su cuenta SIP de Avaya Aura.

Figura 4.101 Interface de Flare Communicator para iPad

b. Puesta en Servicio de Avaya Flare Communicator para Windows

Lo primero que se verifica es la correcta instalación y configuración del aplicativo, cuyas recomendaciones para la PC del usuario son:

- Procesador Dual Core 2.4 GHz
- 2 GB de memoria RAM
- 256MB de memoria RAM para video dedicada
- 1.5 GB de espacio de disco duro libre (mínimo)
- Monitor de alta resolución (1024 x 768)
- Tarjeta de red
- Head Set

Adicionalmente se requiere tener el siguiente software instalado en la PC:

- Microsoft .NET Framework 4
- Microsoft Visual C++ 2005
- Microsoft Visual C++ 2010 x86
- Microsoft DirectX
- Uno de los siguientes sistemas operativos:
  - Microsoft Windows 7 Enterprise Edition (32 bits o 64 bits)
  - Microsoft Windows 7 Ultimate Edition (32 bits o 64 bits)
  - Microsoft Windows 7 Professional Edition (32 bits o 64 bits)
  - Microsoft Windows XP Home Edition (32 bits) con SP3 o superior
  - Microsoft Windows XP Professional Edition (32 bits) con SP3 o superior

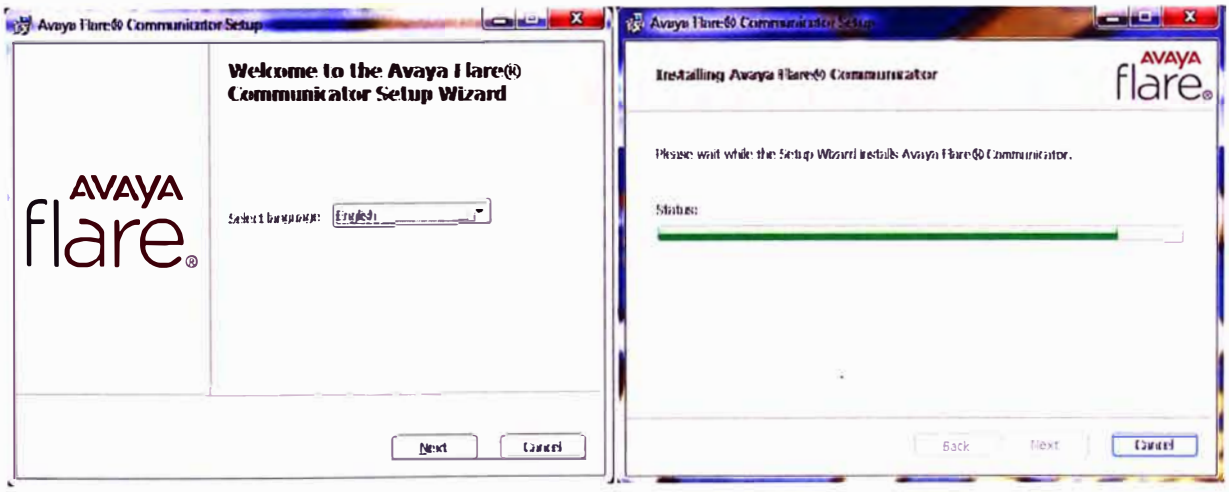


Figura 4.102 Instalación de Flare Communicator para Windows

Luego de haber instalado el Flare Communicator se procede a configurarlo indicando la dirección IP de Avaya Session Manager y Avaya Presence Services, el nombre de dominio, propiedades y reglas de marcación y la integración con el Directorio Activo de la empresa.

Figura 4.103 Configuración de Flare Communicator para Windows

Luego de realizar estas configuraciones retornamos a la ventana de logueo de usuario SIP y está listo para ser utilizado.

Figura 4.104 Interface Flare Communicator para Windows

4.1.11. Puesta en Servicio de Avaya Video Conference Systems 1000 Series

Una vez encendida la cámara de video ingresamos al Menú de Sistema para empezar a configurarla.

Figura 4.105 Pantalla principal de Avaya Video Conference System

Ingresamos al Menú del Sistema y luego ingresamos a Preferencias de Administrado, para lo cual ingresamos la contraseña de administrador.

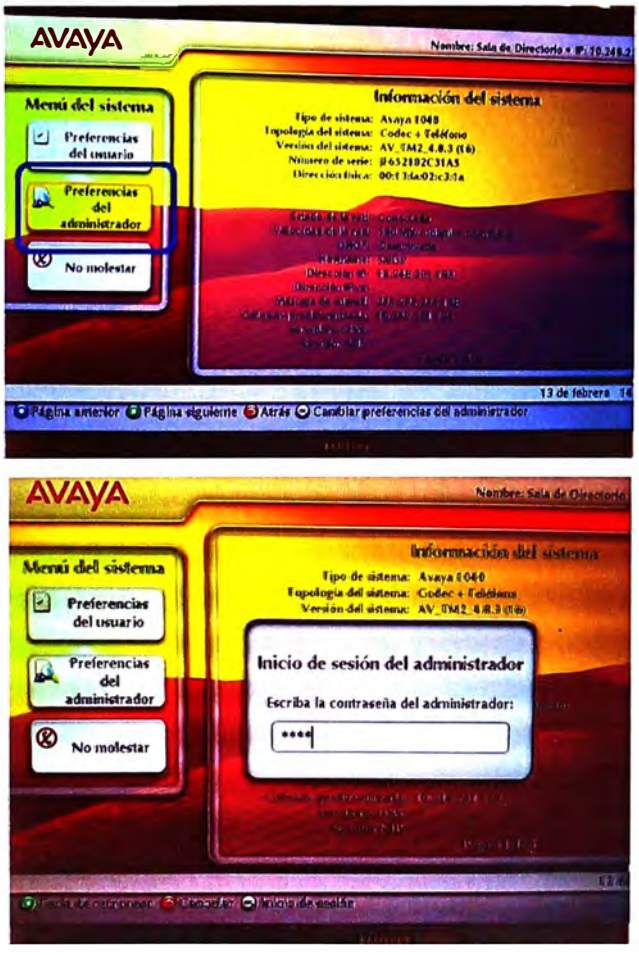


Figura 4.106 Menú de Sistema de Avaya Video Conference System

Dentro de las Preferencias del Administrador encontramos todas las categorías disponibles para las configuraciones del equipo, lo primero que configuramos serán los parámetros de red colocando la dirección IP, máscara de red, Gateway predeterminado, hostname y VLAN del equipo.

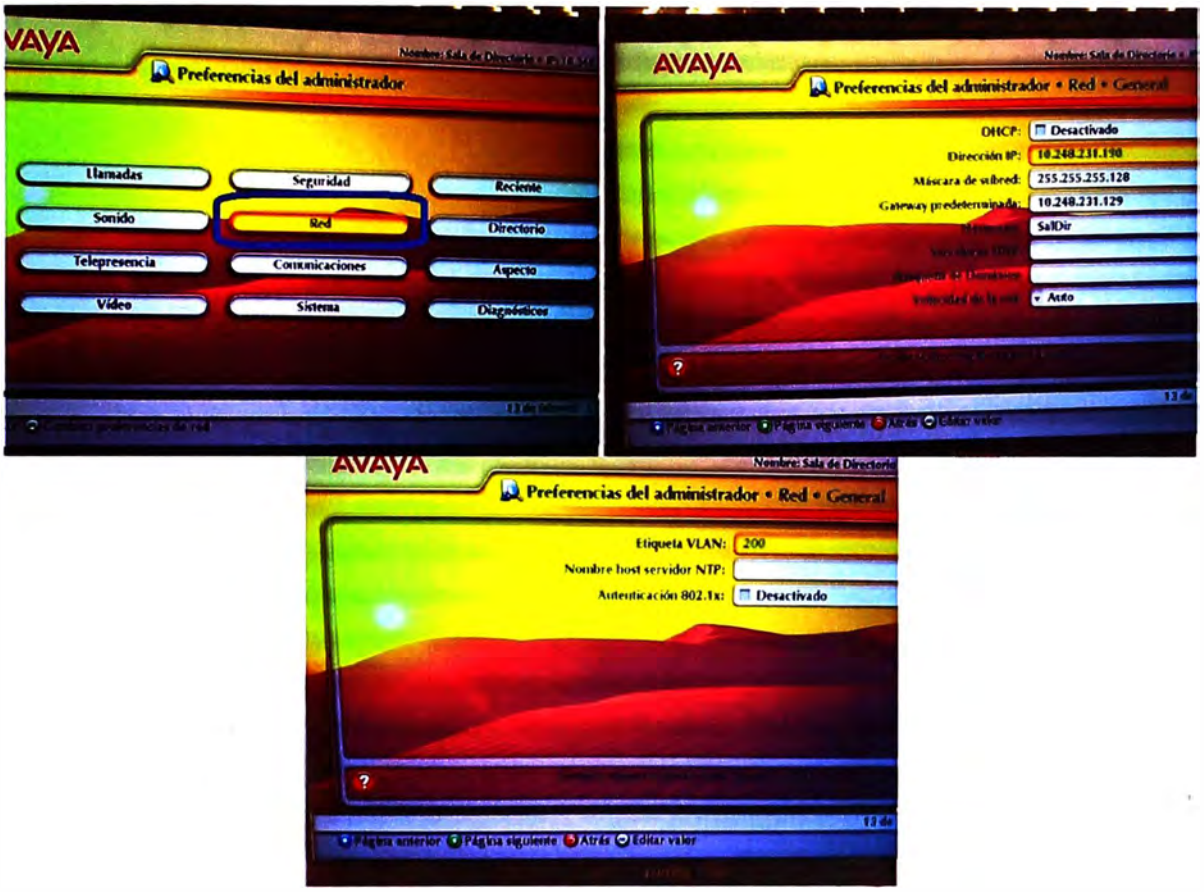
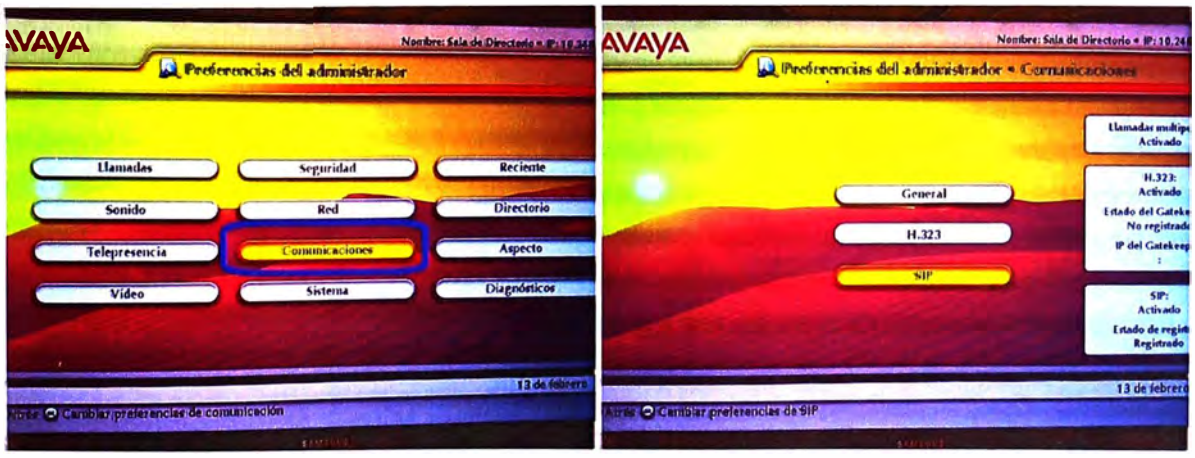


Figura 4.107 Configuración de red de Avaya Video Conference System

Volvemos a Preferencias del Administrador para ingresar a Comunicaciones para configurar todos los parámetros SIP necesarios para que el equipo pueda registrarse en Avaya Session Manager



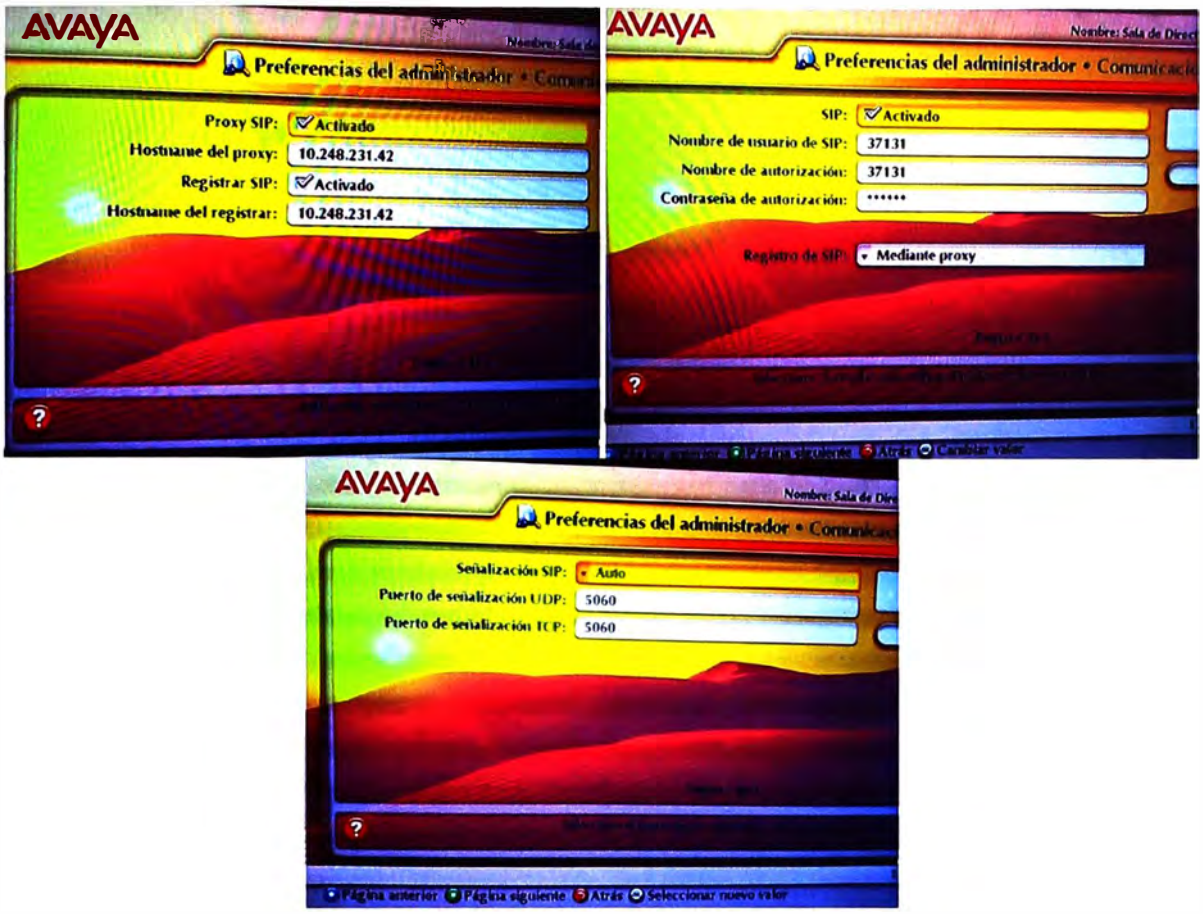


Figura 4.108 Configuración parámetros SIP de Avaya Video Conference System

Hecho esto tenemos el equipo conectado a la red de datos y con los parámetros SIP adecuados para que se pueda registrar en Avaya Session Manager.

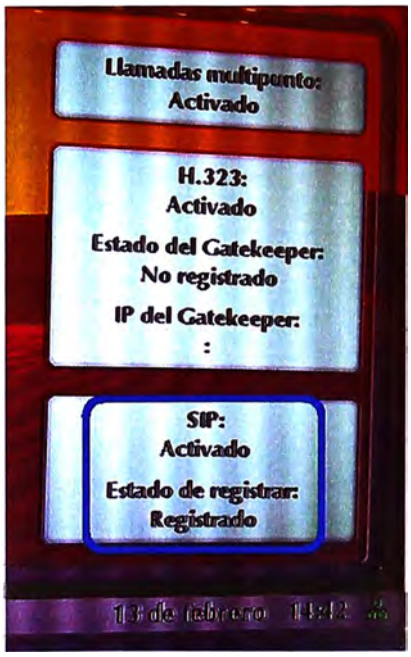


Figura 4.109 Registro SIP de Avaya Video Conference System

4.2. Verificación de Servicios de Avaya Aura

A continuación se verificará que cada servicio mencionado en el presente informe trabaje correctamente.

4.2.1. Verificación de Avaya One-X Deskphone

Lo primero en verificar es la correcta conexión del equipo con Avaya Session Manager utilizando la ventana de logueo del teléfono. El Username y el Password son configurados en el apartado *Manage User* dentro de *User Management*, esto vía web en el Avaya System Manager

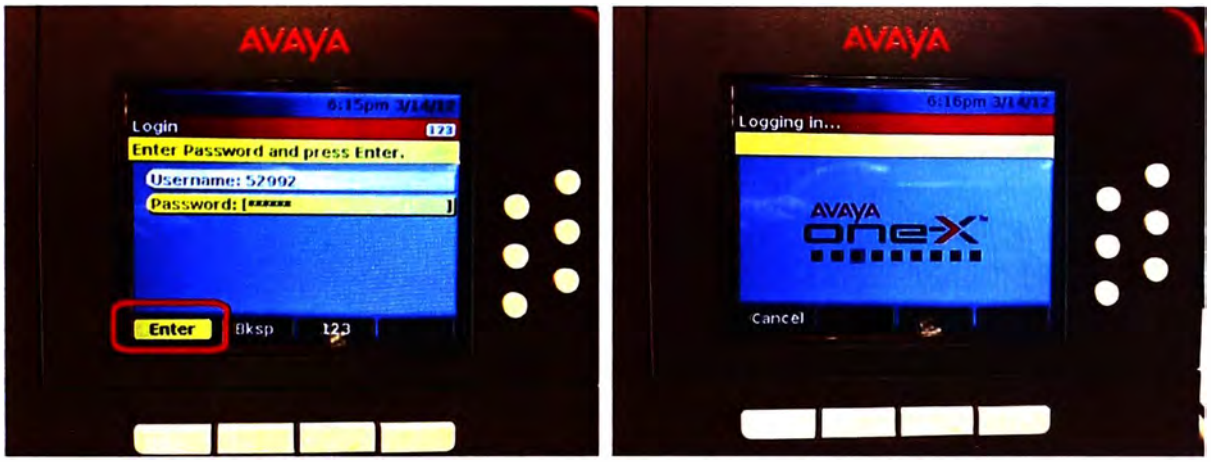


Figura 4.110 Logueo de usuario en Avaya One-X Deskphone

Se verifica la correcta conexión del usuario y que se carguen correctamente sus contactos de Aura, teniendo la posibilidad de llamarlos. Para esto pulsamos la tecla Contacts ubicamos la persona a llamar y pulsamos la tecla Call.

Figura 4.111 Llama simple en Avaya One-X Deskphone

Se verifica la facilidad de transferencia de llamadas pulsando la tecla respectiva durante una llamada en proceso y marcando el destino a donde se enviará dicha llamada. Una vez que el destino contesta la llamada, la transferencia se concreta pulsando la tecla Complete.

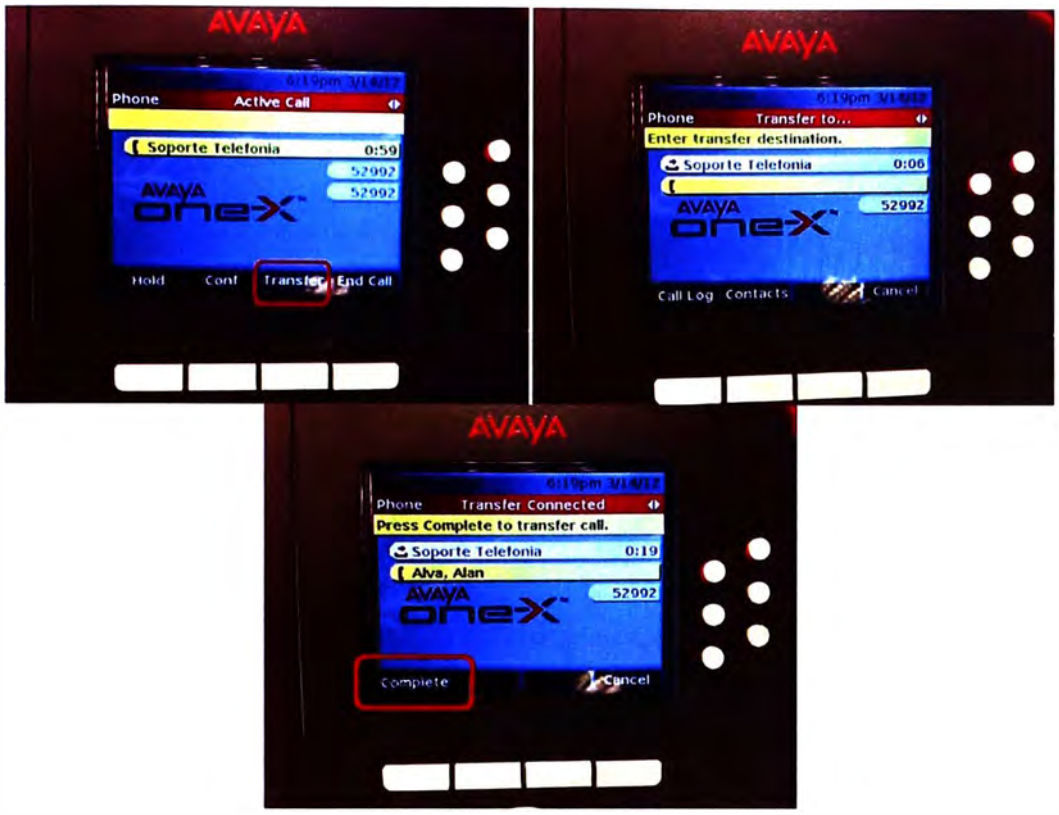


Figura 4.112 Transferencia de llamadas en Avaya One-X Deskphone

Se verifica la facilidad de conferencia pulsando la tecla respectiva durante una llamada en proceso y marcando el número telefónico que queremos adherir a al conversación.

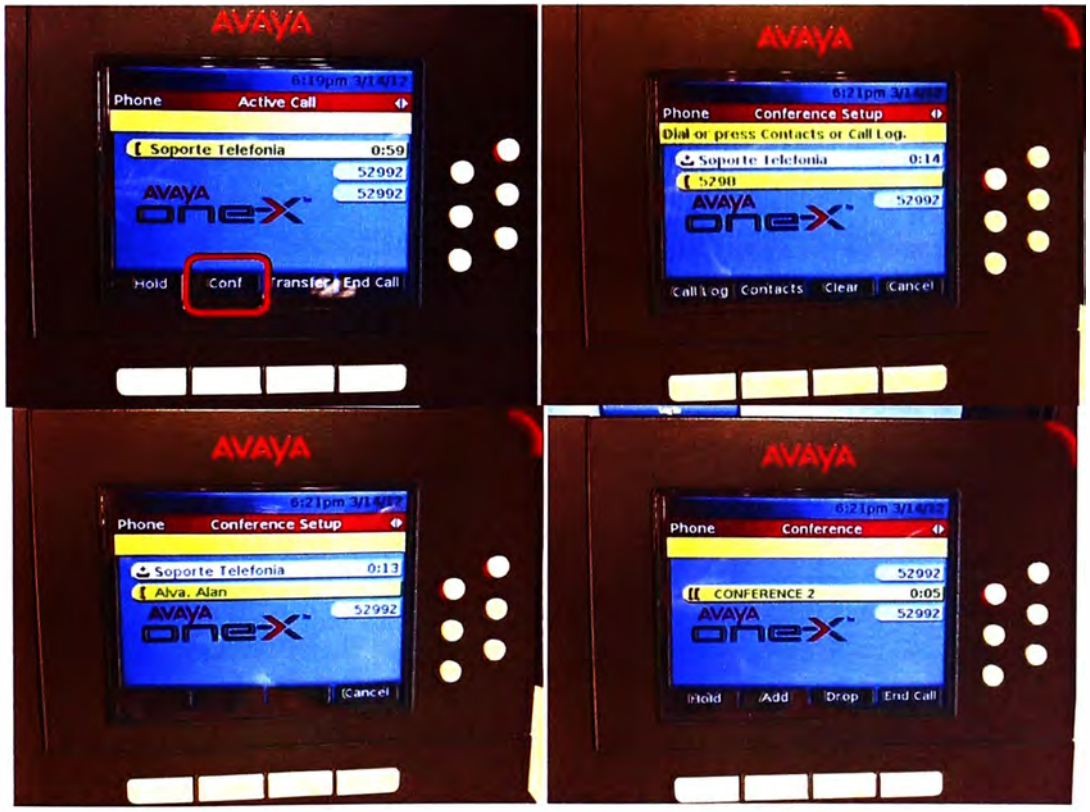


Figura 4.113 Conferencia de voz en Avaya One-X Deskphone

4.2.2. Verificación de Avaya One-X Communicator

Lo primero en verificar es la correcta conexión del aplicativo con Avaya Session Manager para usar los servicios de la Plataforma Aura.

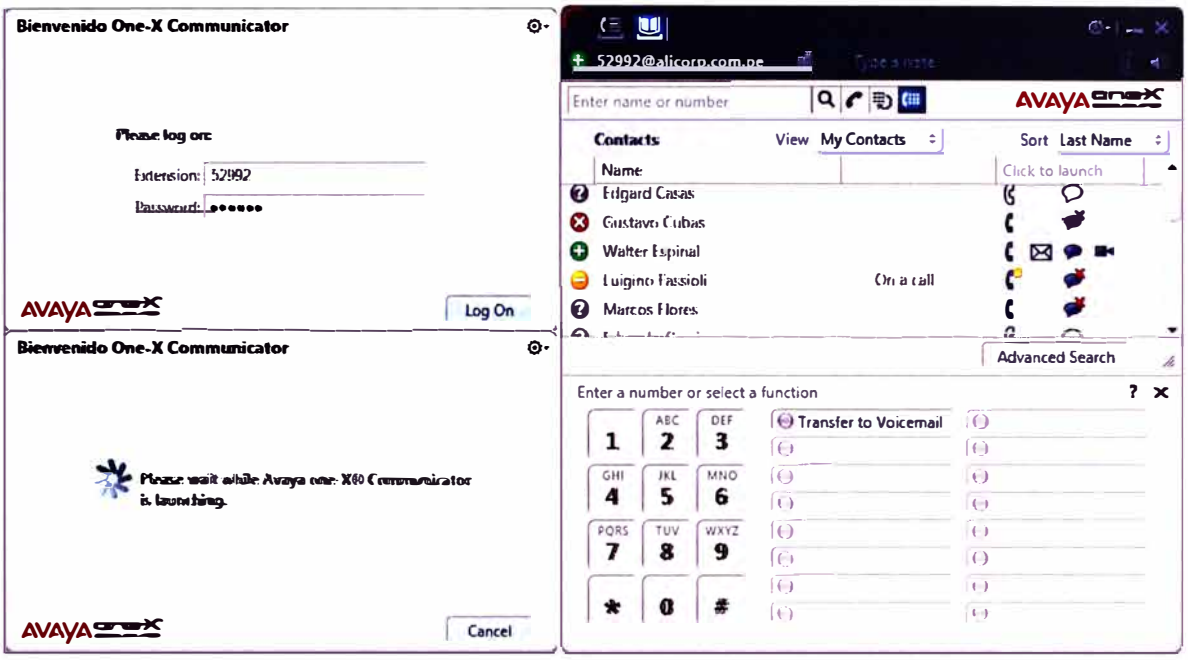


Figura 4.114 Proceso de logueo de usuario de One-X Communicator

Dentro del aplicativo tenemos 2 vistas, la del directorio de contactos y la del registro de llamadas. En el directorio de contactos podemos ver el estado de presencia de los contactos y los medios que tenemos a disposición para comunicarnos con ellos (llamada de voz, llamada de audio o mensajería instantánea) dando sólo un clic en la opción requerida.

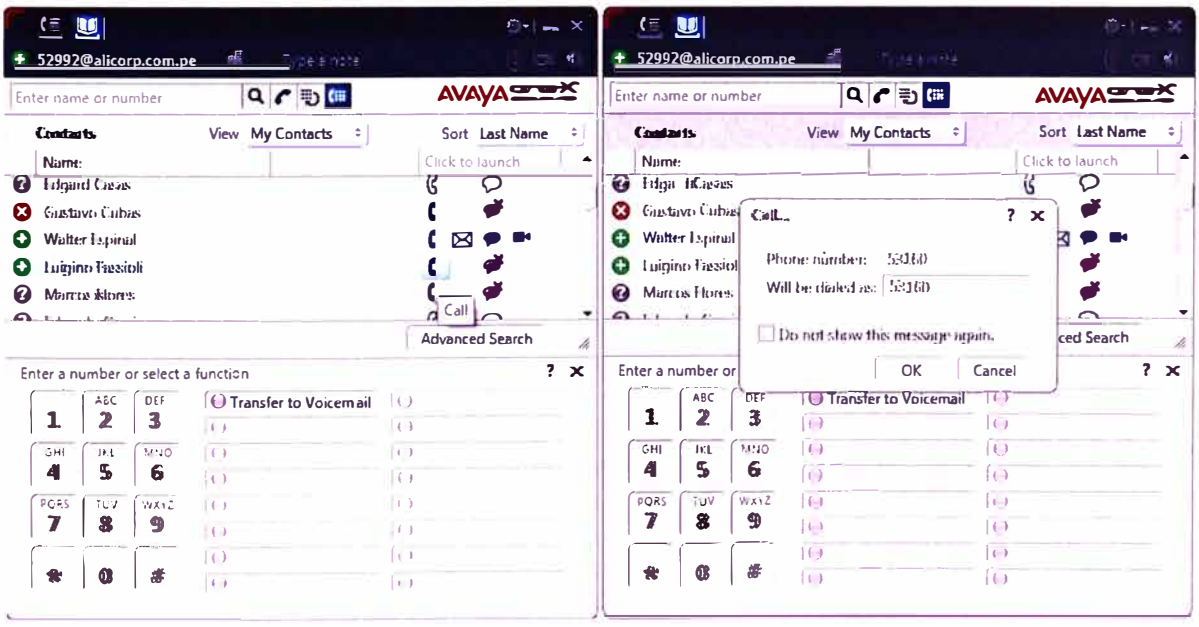


Figura 4.115 Llamada realizada desde de One-X Communicator

Estando ya con la llamada en curso se puede verificar la facilidad de Conferencia con el botón respectivo y luego especificando el número del teléfono con el que queremos hacer la conferencia.

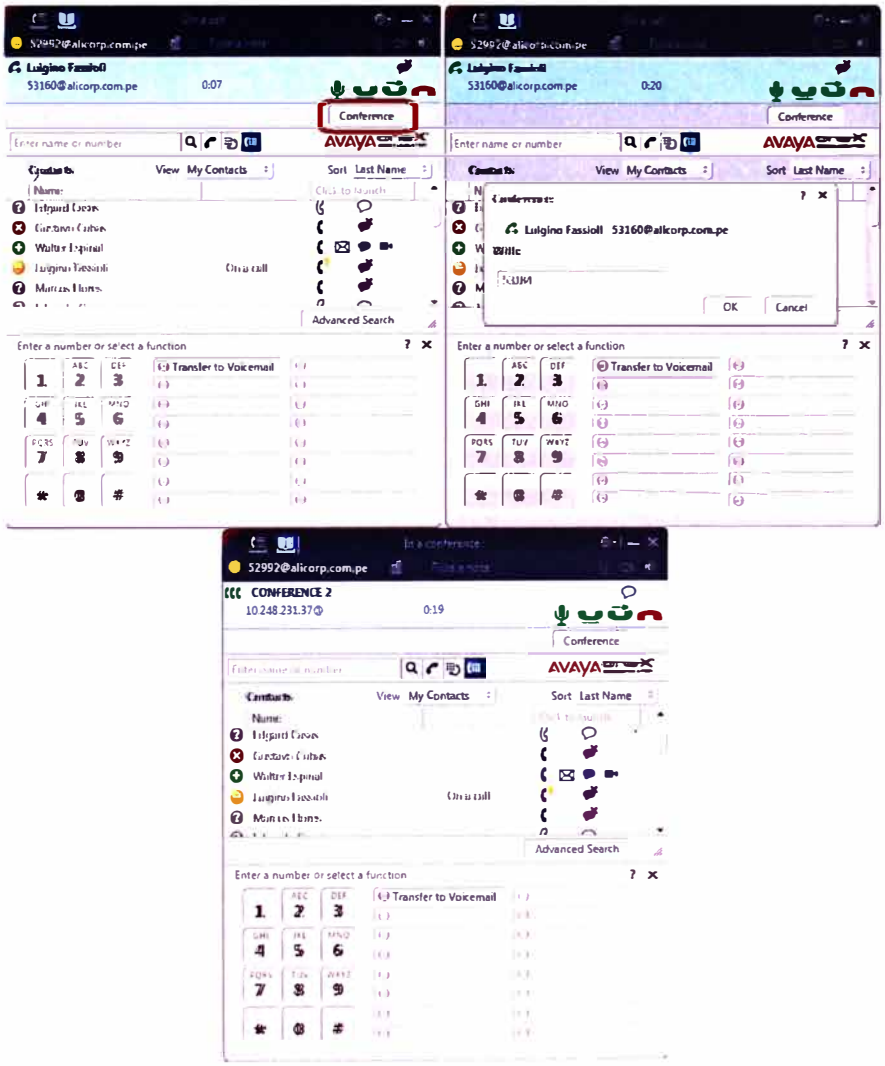


Figura 4.116 Conferencia de Voz en One-X Communicator

Se verifica también la transferencia de una llamada en curso con el botón respectivo luego especificando el número del teléfono con el que queremos hacer la transferencia. Al confirmar el destino la llamada es transferida y desaparece de nuestro One-X Communicator.

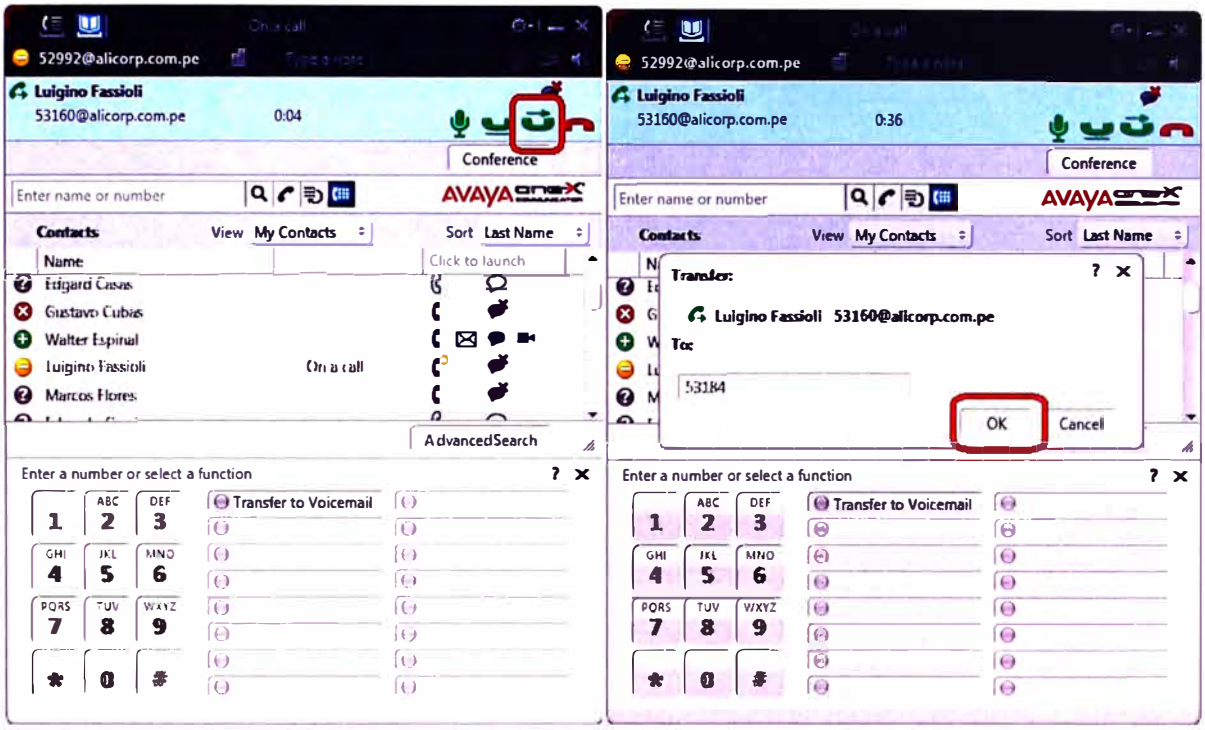


Figura 4.117 Transferencia de llamada en One-X Communicator

Tal como mencionamos anteriormente, la segunda vista del One-X Communicator era el historial de llamadas. Se verifica el registro de las llamadas entrantes, salientes y perdidas y la opción de poder marcar los números telefónicos guardados en este historial. En la figura vemos la devolución de una llamada perdida.

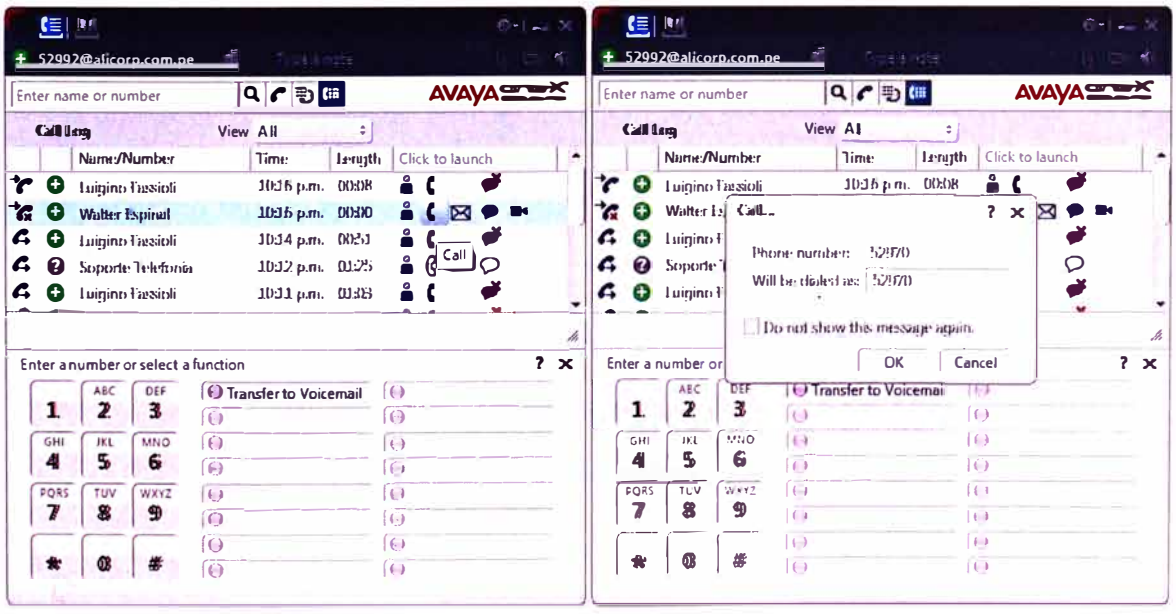


Figura 4.118 Manejo del registro de llamadas en One-X Communicator

Se verifican las llamadas hacia números telefónicos que no tengamos registrados como contactos ya sean números corporativos o externos usando casilla de marcación.

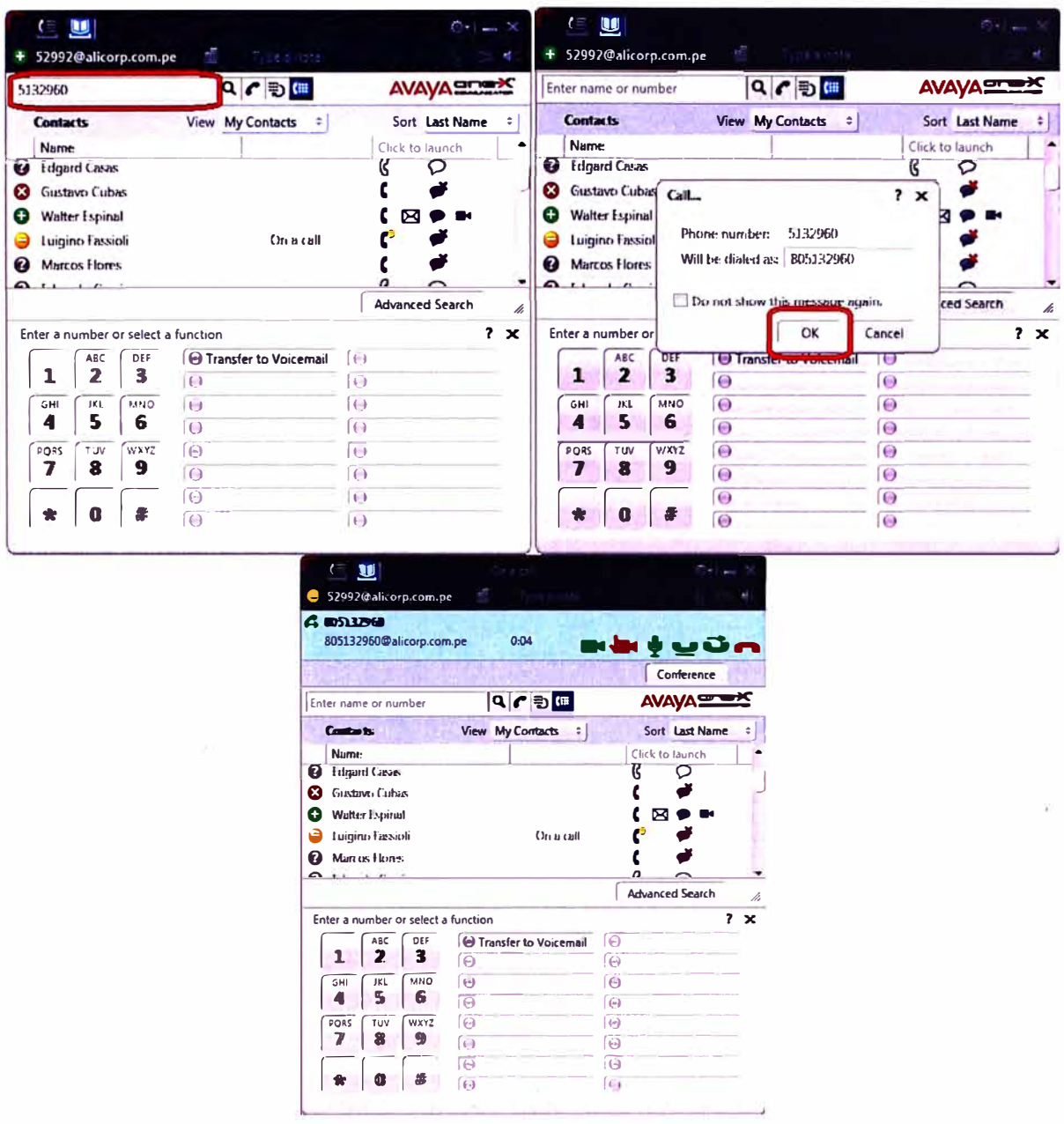


Figura 4.119 Marcado de números específicos en One-X Communicator

Finalmente se muestra el flujo de las llamadas hechas utilizando el One-X Communicator a números corporativos y externos. Nuestra PC utiliza la señal wifi del local donde nos encontremos situados y si activamos el One-X Communicator dicha PC se convierte en una estación SIP registrada en la Plataforma Avaya Aura y utiliza a Avaya Communication Manager para llamar al número telefónico deseado. En el caso que el usuario se encuentre fuera de la Red Corporativa tendría que utilizar una conexión VPN para conectarse a la plataforma, en el caso que el usuario sí se encuentre dentro de la Red Corporativa el uso de una VPN no sería necesario.

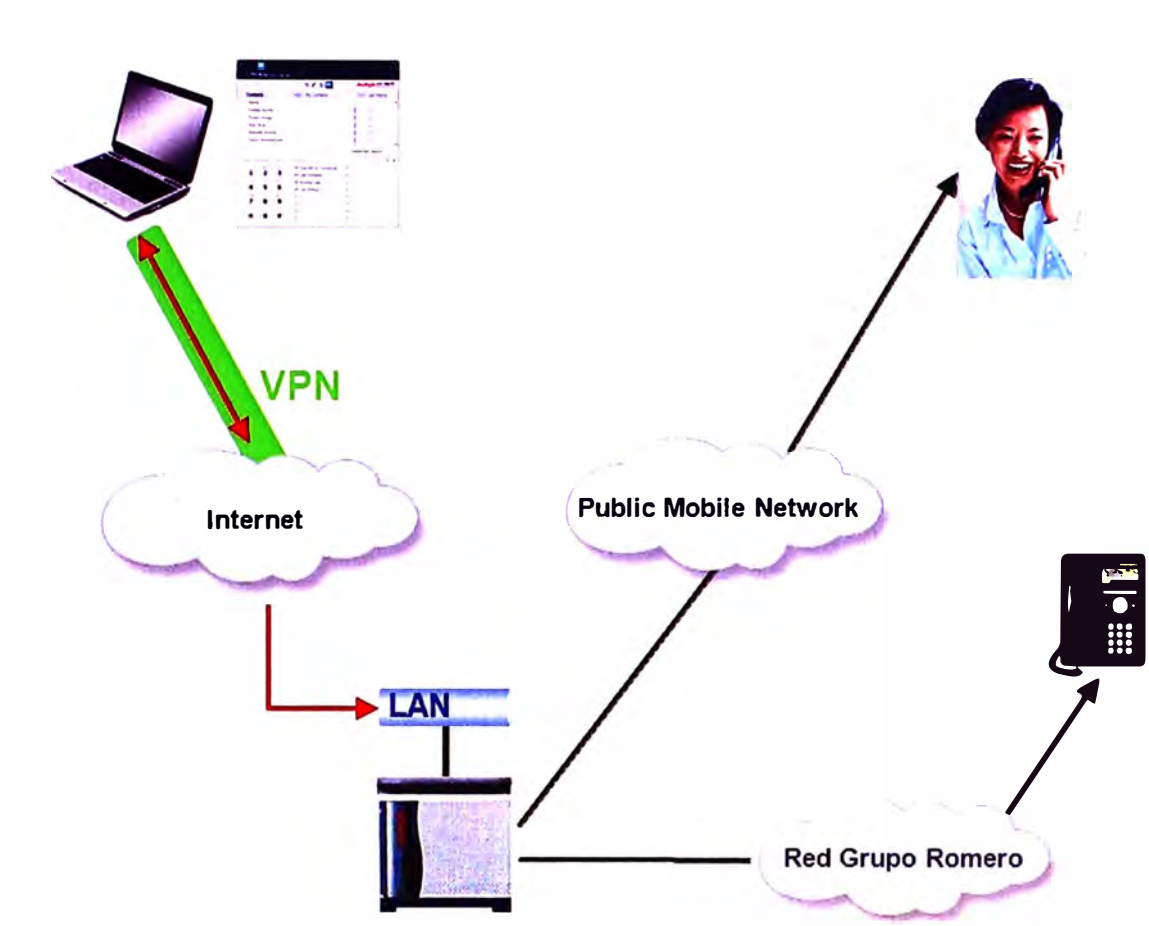


Figura 4.120 Diagrama de flujo para realizar llamadas con One-X Communicator.

4.2.3. Verificación de Avaya One-X Mobile

Lo primero en verificar es la correcta conexión del dispositivo móvil a la Plataforma Aura, para lo cual se ingresa el usuario y contraseña respectiva respectiva, así como los datos de servidor y puerto a utilizar.

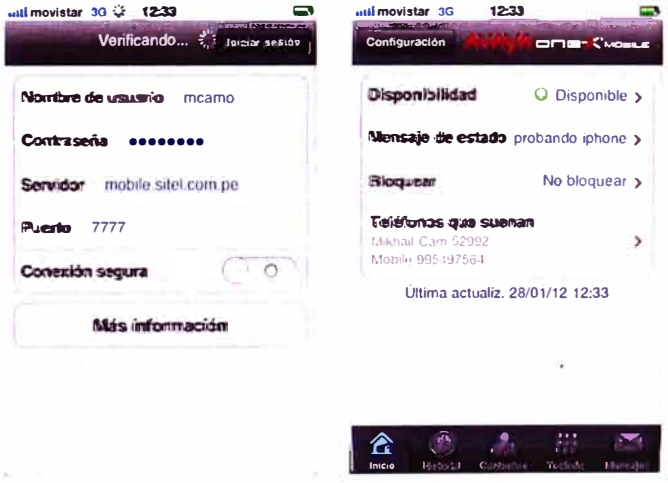


Figura 4.121 Logueo de usuario en One-X Mobile

Se verifica una llamada a un anexo del Grupo usando el One-X Mobile. La orden de la llamada es enviada por el servicio 3G de nuestro móvil hacia el servidor One-X CES que tiene el Grupo. El servidor One-X CES le da la orden al Communication Manager de llamarnos en primer lugar a nuestro móvil 995497564, esta llamada la recibimos por una

de las líneas celulares licea del Grupo para ahorrar costo, al responder esta llamada de retorno (callback) el Communication Manager hace la llamada al destino deseado, en este caso el anexo 53184 y nos conecta con él.

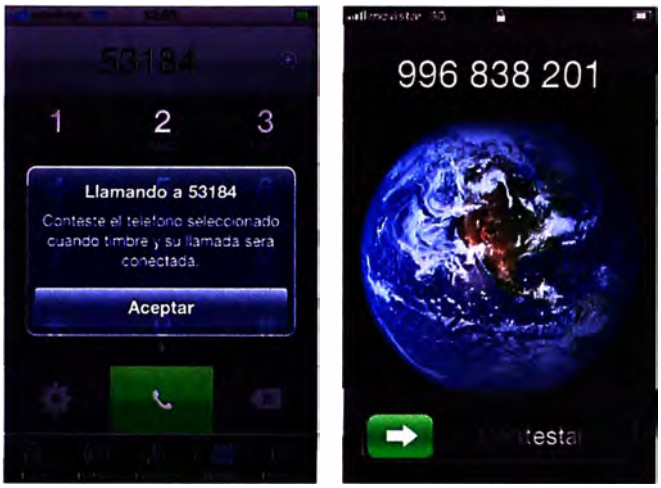


Figura 4.122 Llamada usando One-X Mobile

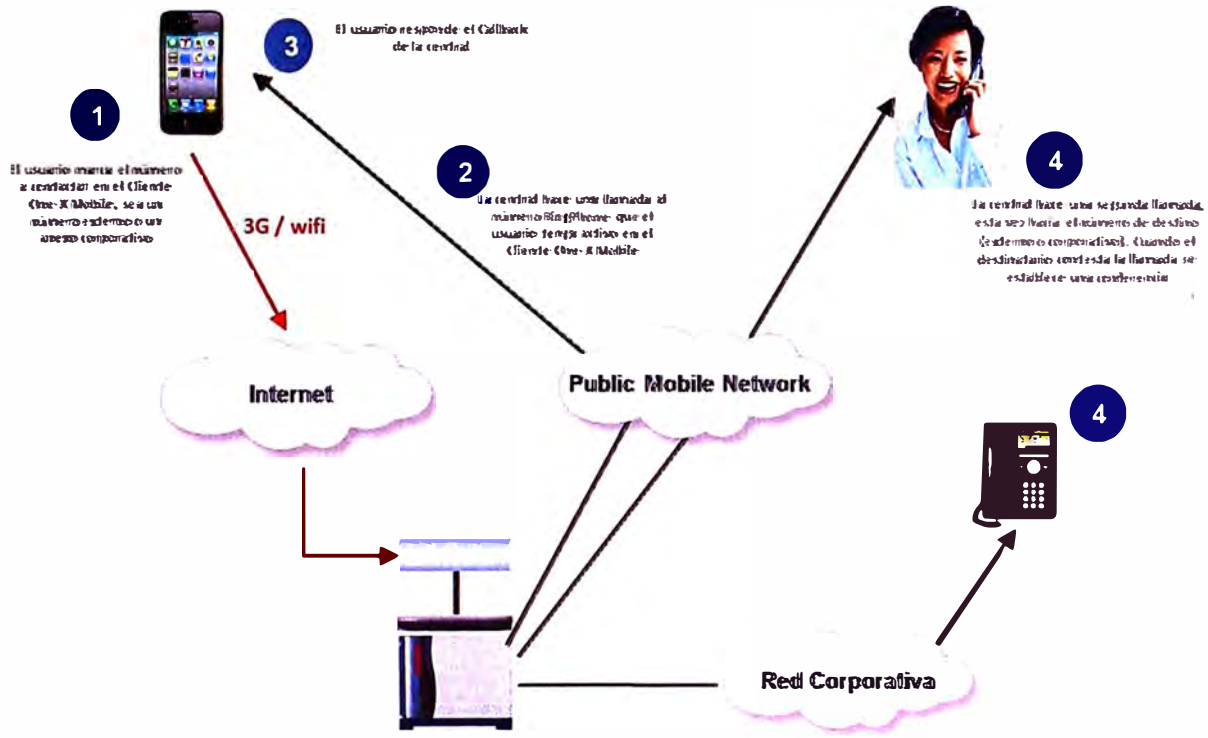


Figura 4.23 Diagrama de flujo para realizar llamadas con One-X Mobile

Se verifica la notificación en el caso que tengamos un mensaje de voz en la casilla de nuestro anexo viendo el aviso en el ícono respectivo, ingresamos a la categoría Mensajes y veremos el listado de todos los mensajes de voz presentes en nuestra casilla, podemos escoger el que deseamos reproducir para oírlo, luego tenemos la posibilidad de eliminar el mensaje o de responder con una llamada hacia el número del usuario que nos dicho mensaje.

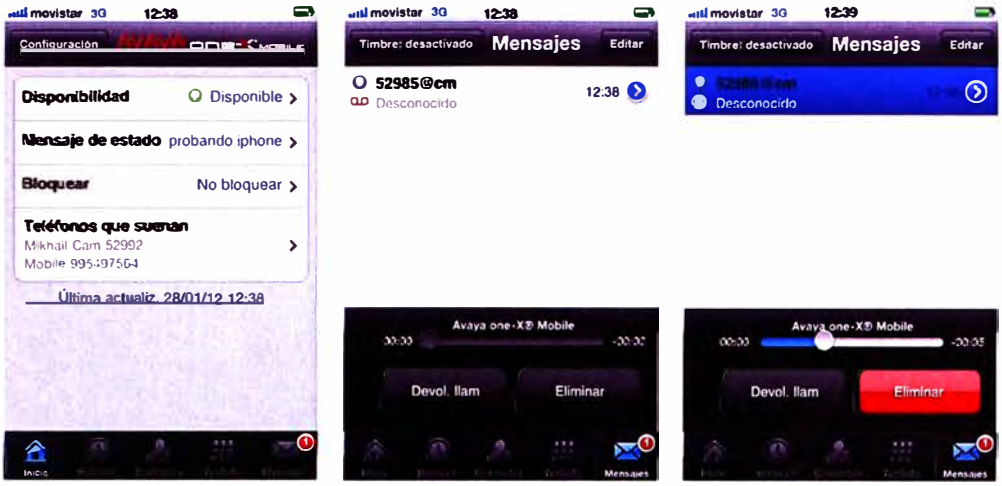


Figura 4.124 Manejo de Casilla de Voz en One-X Mobile

Se verifica el registro correcto de las llamadas salientes y entrantes, contestadas o perdidas, teniendo opción de llamar a estos números.

Figura 4.125 Manejo de registro de llamadas en One-X Mobile

Se verifica el manejo del estado de presencia de nuestro anexo desde el equipo móvil ya sea en forma manual o automática.

Figura 4.126 Manejo de presencia en One-X Mobile

Se verifica la facilidad del manejo de restricción de llamadas entrantes. Por defecto el cliente One-X Mobile del móvil recibe todas las llamadas que lleguen al anexo en nuestro sitio de trabajo; adicionalmente podemos escoger recibir sólo las llamadas procedentes de determinados contactos VIP o hasta quizás bloquear todas las llamadas que nuestro anexo reciba cuando no deseemos atenderlas.

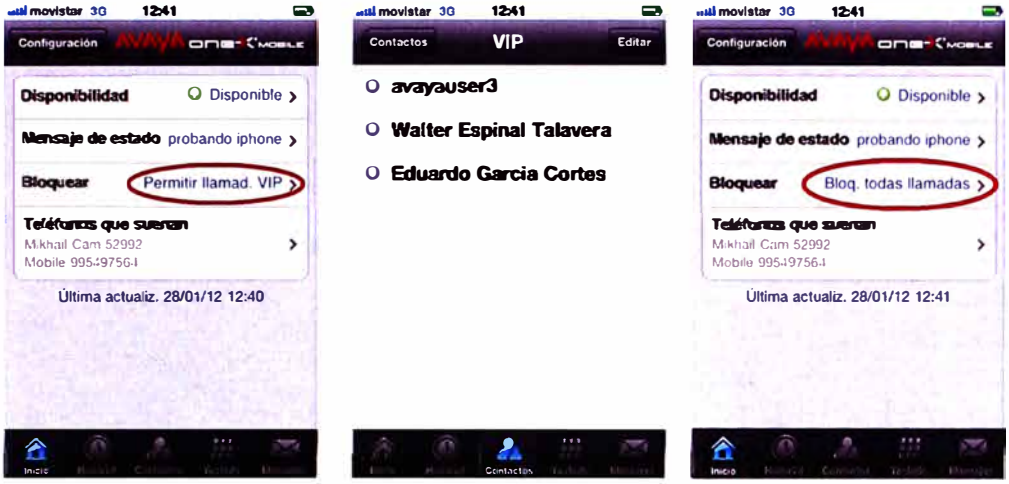


Figura 4.127 Restricción de llamadas entrantes en One-X Mobile

Se verifica el manejo de los teléfonos de timbrado (Ring Phone) ingresando a la categoría respectiva en el menú principal del cliente One-X Mobile y activando o desactivando los números en donde quisiéramos que la Plataforma Aura nos ubique cuando no podamos contestar llamadas en nuestro teléfono de escritorio, adicionalmente a nuestro equipo móvil podemos agregar quizás algún teléfono externo o quizás algún otro anexo corporativo. La Plataforma Aura hará un timbrado simultáneo a los números que se encuentren activos al momento de la llamada.

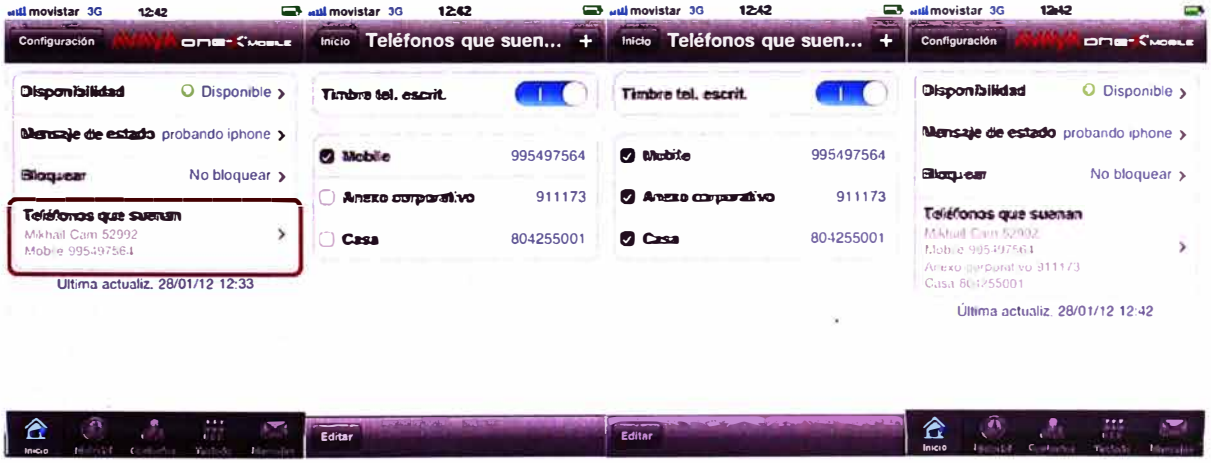


Figura 4.128 Activación de teléfonos de timbrado (Ring Phones) en One-X Mobile

4.2.4. Verificación de Servicio de Avaya Desktop Video Device

Lo primero en verificar es la correcta conexión del Avaya Desktop Video Device (ADVD) con Avaya Session Manager para usar los servicios de la Plataforma Aura.

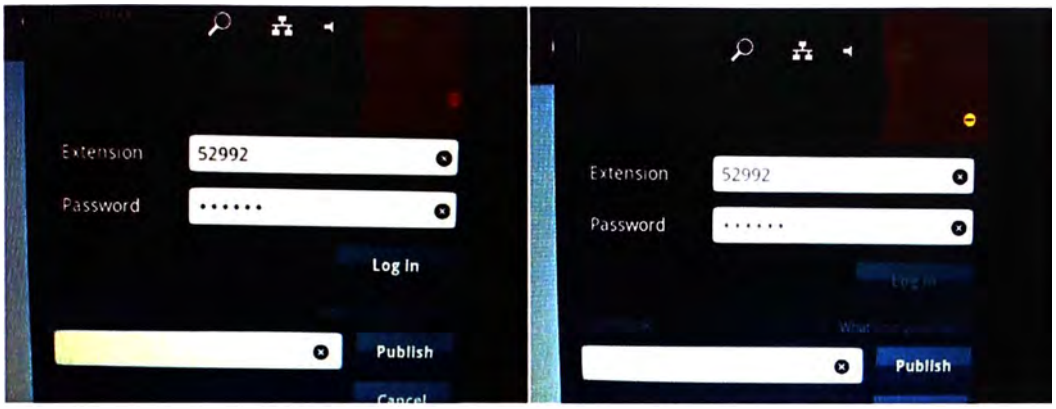


Figura 4.129 Logueo de usuario en Avaya Desktop Video Device

Una vez iniciada la sesión se verifica que se cargan correctamente los contactos del usuario en el lado derecho de la pantalla y las cuentas de correo electrónico y Facebook se actualizan de manera correcta en la parte superior izquierda.

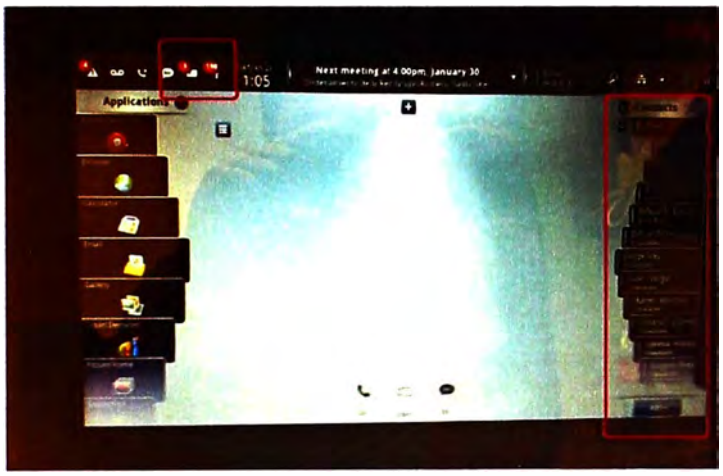


Figura 4.130 Interface de Operación de Avaya Desktop Video Device

Se verifica la correcta publicación de los estados de presencia de nuestros contactos y saber con esto por qué medios podemos contactar a cada uno.

Figura 4.131 Estados de Presencia en Avaya Desktop Video Device

Se verifica la facilidad de explorador web desde el Avaya Desktop Video Device (ADVD) utilizando la opción correspondiente en la parte izquierda de la pantalla.

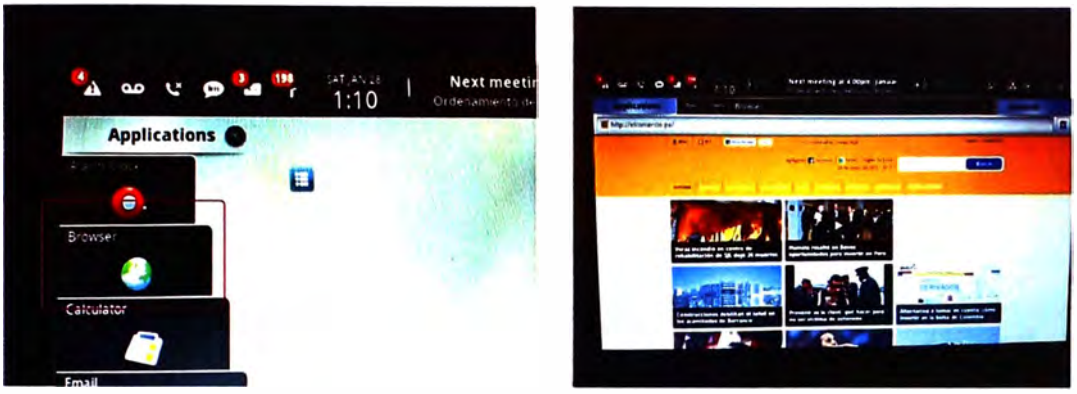


Figura 4.132 Exploración web de Avaya Desktop Video Device

Se verifica la correcta sincronización de las cuentas de correo configuradas en el Avaya Desktop Video Device (ADVD) así como la Agenda de la cuenta de correo corporativa del usuario.

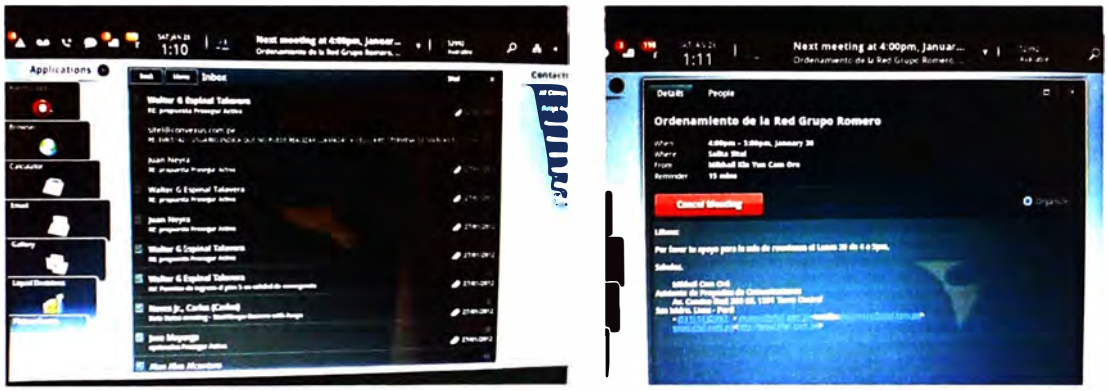


Figura 4.133 Sincronización de Cuenta de Correo
y Agenda en Avaya Desktop Video Device

Se verifica la función de manejo de las cuentas de correo electrónico configuradas en e equipo pudieron leer, responder o renviar los correos con el apoyo de un teclado táctil.

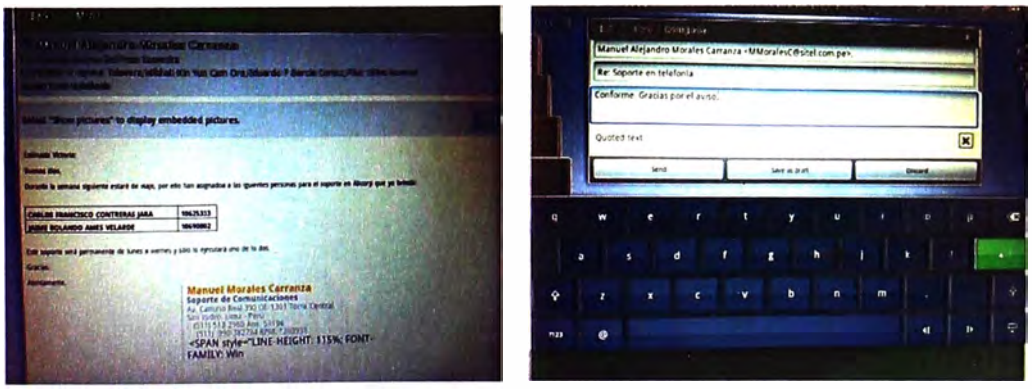


Figura 4.134 Manejo de Cuenta de Correo en Avaya Desktop Video Device

Se verifica de igual manera la correcta visualización de los documentos adjuntos en los correos revisados en el Avaya Desktop Video Device.

Figura 4.135 Visualización de archivos adjuntos en Avaya Desktop Video Device

Se verifica la correcta sincronización de la cuenta de Facebook configurada en el Avaya Desktop Video Device (ADVD) mostrando las actualizaciones de los contactos del usuario.

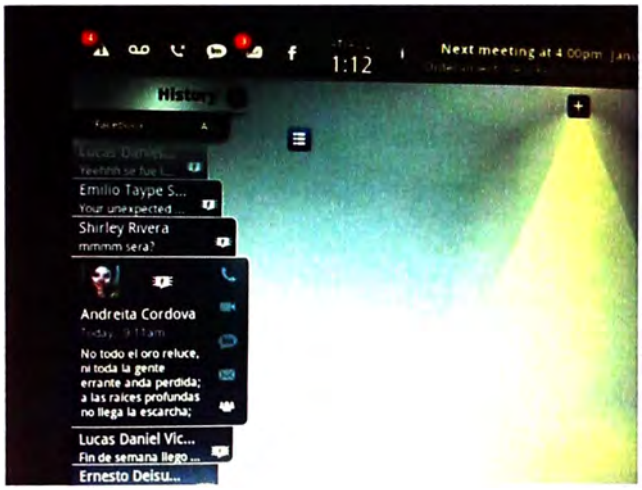


Figura 4.136 Actualizaciones de contactos Facebook en Avaya Desktop Video Device

Se verifica el correcto establecimiento de las llamadas de voz entre anexos corporativos con el teclado táctil del Avaya Desktop Video Device (ADVD).

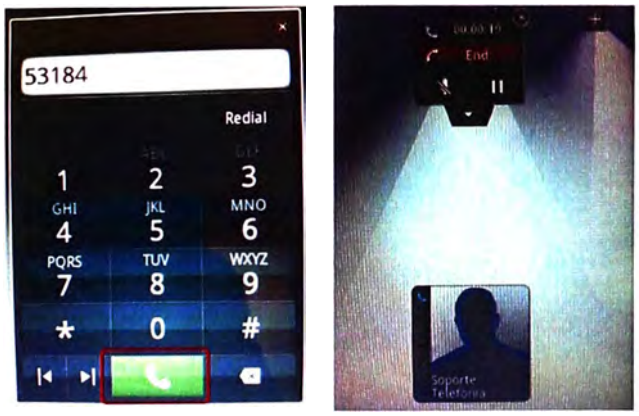


Figura 4.137 Establecimiento de llamadas en Avaya Desktop Video Device

Entablada la llamada de voz se verifica que el usuario puede contestar cualquier llamada que ingrese al equipo en ese mismo instante, o si desea puede realizar una 2da llamada simultánea. En cualquiera de los 2 casos mencionados la primera llamada queda en espera colocada en al lado de la pantalla y la podemos derivar o transferir según lo que necesitemos con solo devolverla a la parte central de la misma.

Figura 4.138 Desvío y Transferencia de llamadas en Avaya Desktop Video Device

4.2.5. Verificación de Servicio de Avaya Flare Communicator

Se verifica a continuación que ambas versiones de Flare Communicator (para iPad y para Windows) funcionen correctamente. Este aplicativo es ideal para los usuarios que necesitan movilidad y desean conectarse frecuentemente desde fuera de la red del Grupo Empresarial. Para estos usuarios el flujo de las llamadas es el mismo para ambas versiones de Flare Communicator existentes, el cual se grafica a continuación.

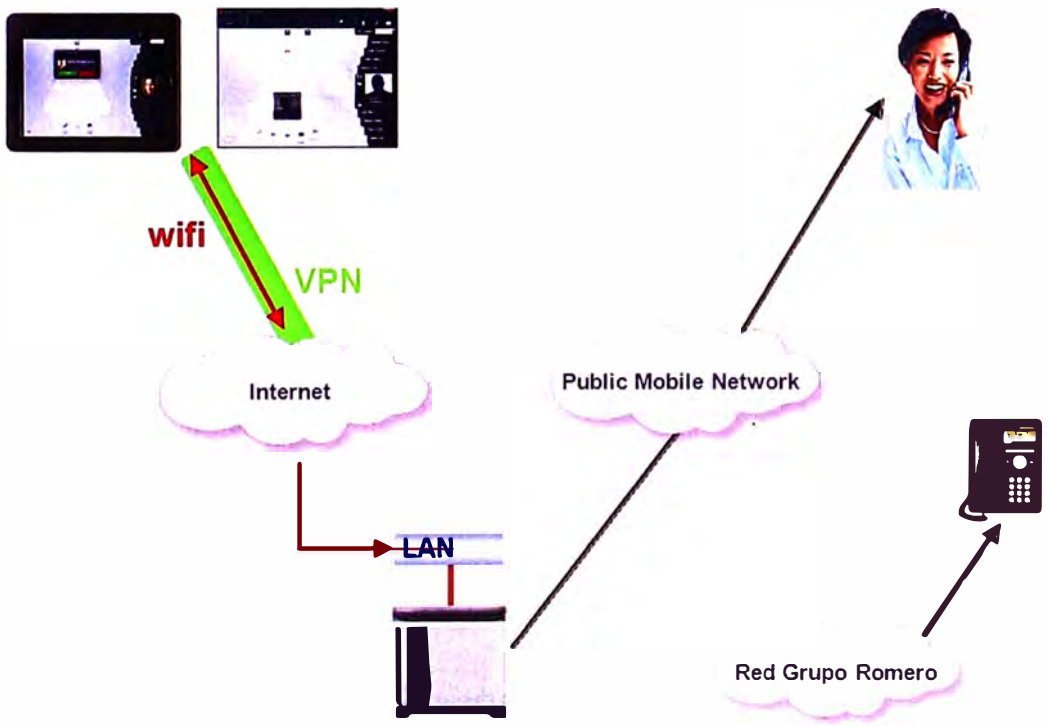


Figura 4.139 Flujo de llamadas en Avaya Flare Communicator

a. Verificación de Servicio de Avaya Flare Communicator para iPad

Lo primero en verificar es la correcta conexión del Avaya Flare Communicator con Avaya Session Manager para usar los servicios de la Plataforma Aura.

Figura 4.140 Logueo de usuario en Avaya Flare Communicator para iPad

Una vez conectados a Avaya Session Manager verificamos que los contactos de nuestra cuenta SIP y de nuestra cuenta local de correo son cargados correctamente y podemos ver sus ficha de contacto indicándonos los medios disponibles para comunicarnos con ellos. Se verifica el servicio con llamadas de prueba desde el directorio de contactos.

Figura 4.141 Llamada a contacto en Avaya Flare Communicator para iPad

Se verifica el servicio de llamadas telefónicas marcando el número de destino desde el teclado de aplicativo.

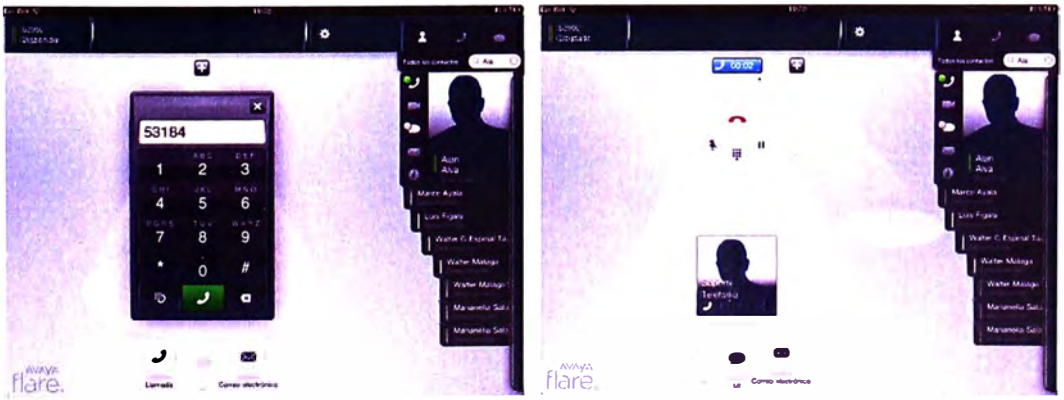


Figura 4.142 Llamada marcando teclado en Avaya Flare Communicator para iPad

Se verifica el manejo de una segunda llamada al poder poner "en espera" a la llamada activa, la cual se hace a un lado en la pantalla de aplicativo y deja la posición central a la segunda llamada, posteriormente tenemos opción de retomarla.

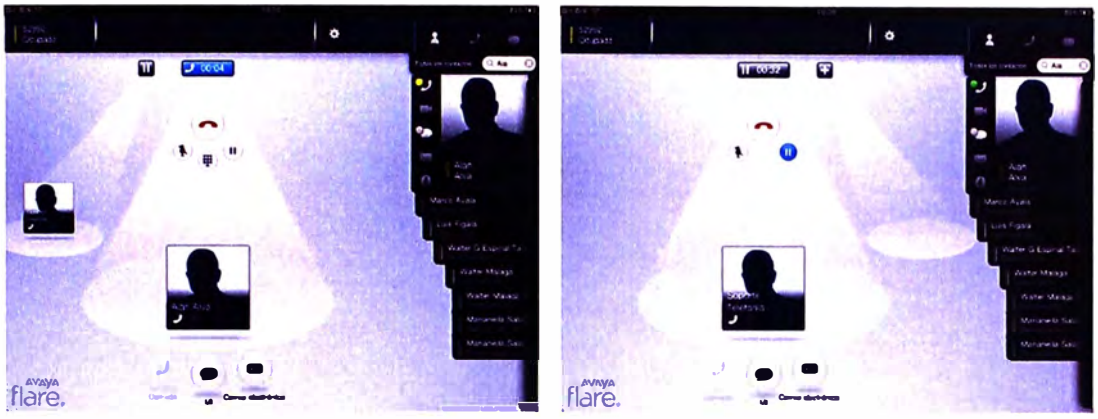


Figura 4.143 Llamada "en espera" en Avaya Flare Communicator para iPad

Se verifica el registro de llamadas entrantes, salientes y perdidas, pudiendo marcar directamente a los números de cada registro.

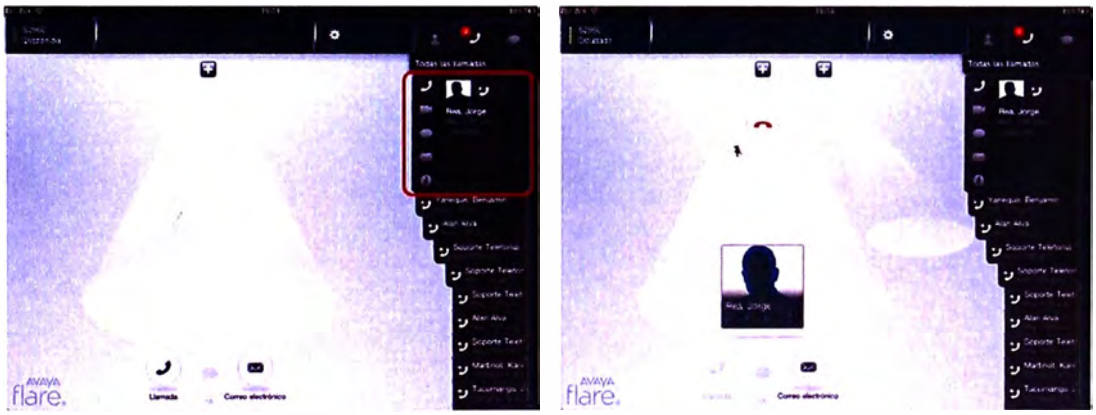


Figura 4.144 Registro de llamadas en Avaya Flare Communicator para iPad

Finalmente se verifica la integración del aplicativo con la cuenta de correo configurada localmente en el iPad, elegimos el contacto de destino, elegimos enviarle un correo y lo enviamos sin necesidad de salir de Flare Communicator y entrar al correo del iPad.

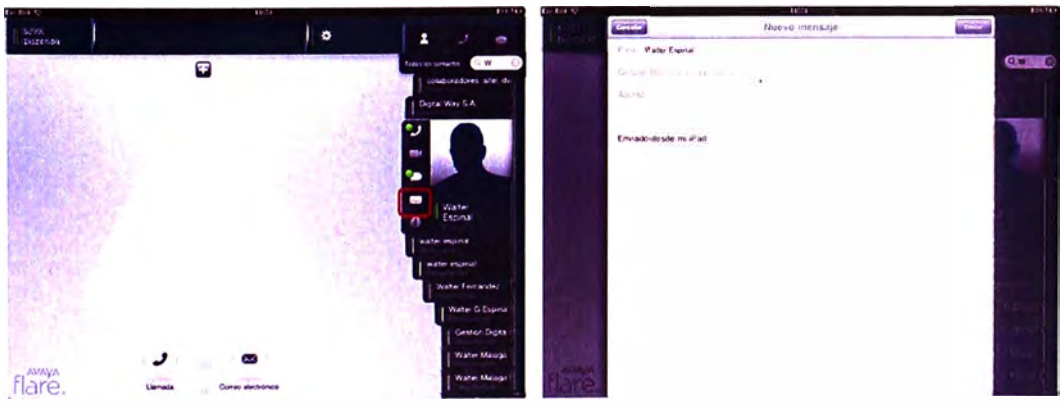


Figura 4.145 Envío de correos desde Avaya Flare Communicator para iPad

b. Verificación de Servicio de Avaya Flare Communicator para Windows

Lo primero en verificar es la correcta conexión del Avaya Flare Communicator con Avaya Session Manager para usar los servicios de la Plataforma Aura.

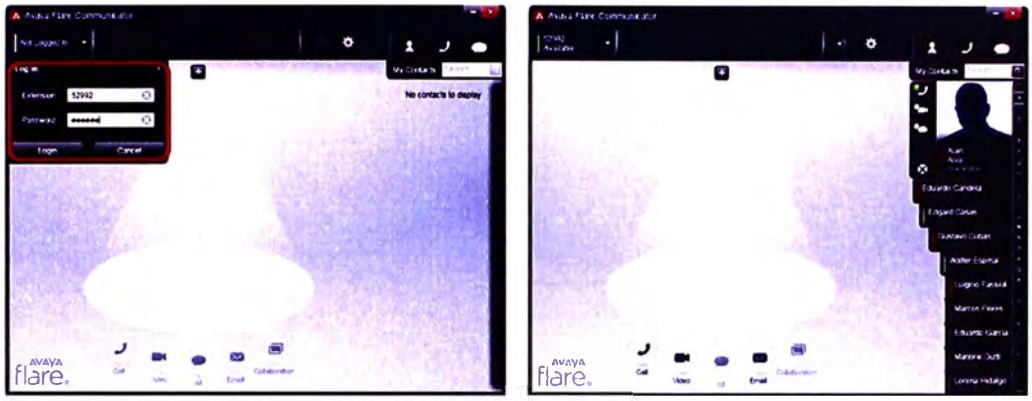


Figura 4.146 Logueo de usuario en Avaya Flare Communicator para Windows

Una vez conectados a Avaya Session Manager verificamos que los contactos de nuestra cuenta SIP y de nuestra cuenta local de correo son cargados correctamente y podemos ver sus ficha de contacto indicándonos los medios disponibles para comunicarnos con ellos. Se verifica el servicio con llamadas de prueba desde el directorio de contactos.

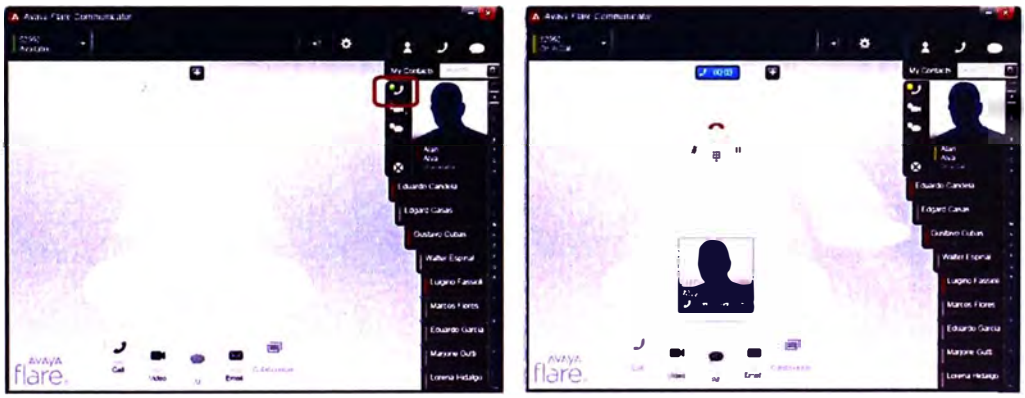


Figura 4.147 Llamada a contacto en Avaya Flare Communicator para Windows

Se verifica el servicio de llamadas telefónicas marcando el número de destino desde el teclado de aplicativo.

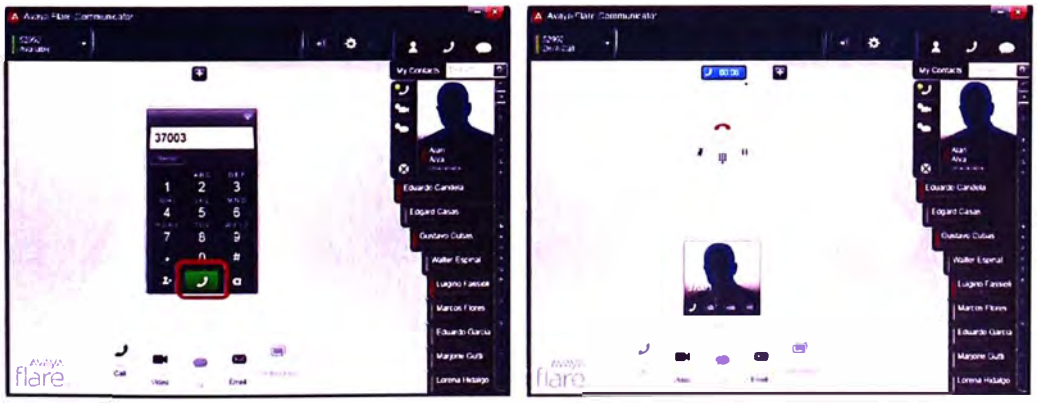


Figura 4.148 Llamada marcando teclado en Avaya Flare Communicator para Windows

Se verifica el manejo de una segunda llamada al poder poner "en espera" a la llamada activa, la cual se hace a un lado en la pantalla de aplicativo y deja la posición central a la segunda llamada, posteriormente tenemos opción de retomarla.

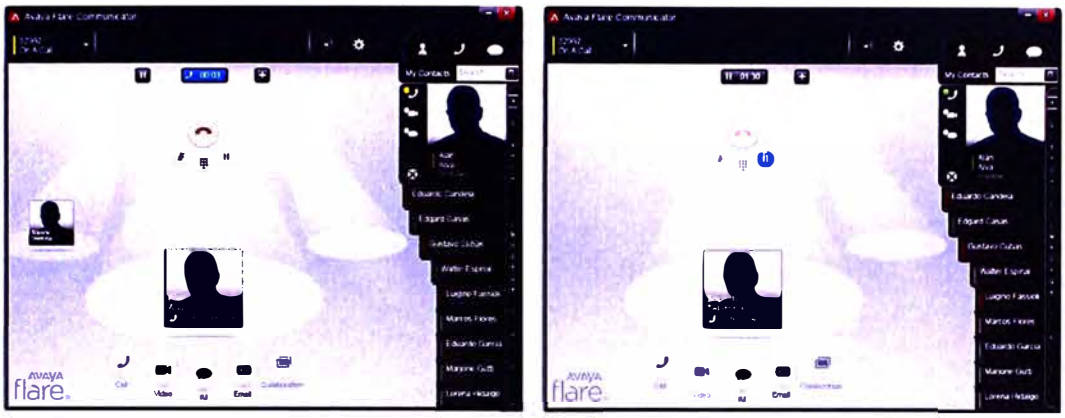


Figura 4.149 Llamada "en espera" en Avaya Flare Communicator para Windows

Se verifica el registro de llamadas entrantes, salientes y perdidas, pudiendo marcar directamente a los números de cada registro.

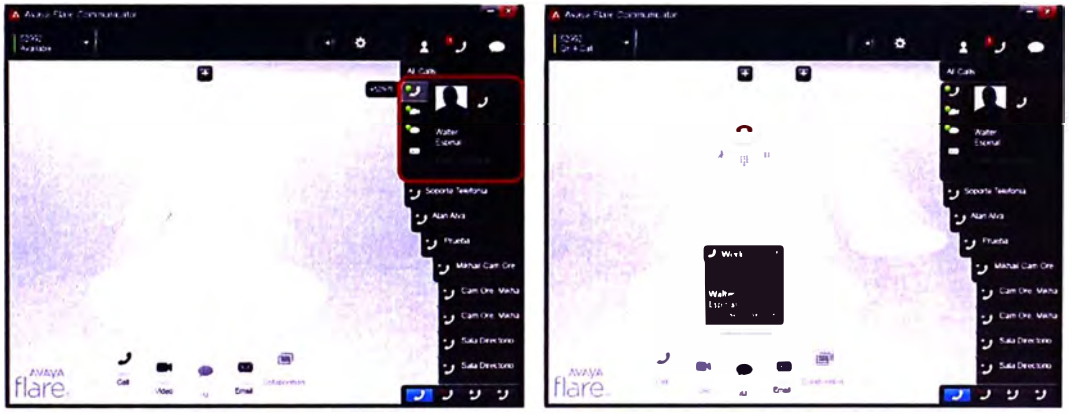


Figura 4.150 Registro de llamadas en Avaya Flare Communicator para Windows

Finalmente se verifica la integración del aplicativo con la cuenta de correo configurada localmente en el Microsoft Outlook, elegimos el contacto de destino, elegimos enviarle un correo y lo enviamos sin necesidad de salir de Flare Communicator y entrar al correo del iPad.

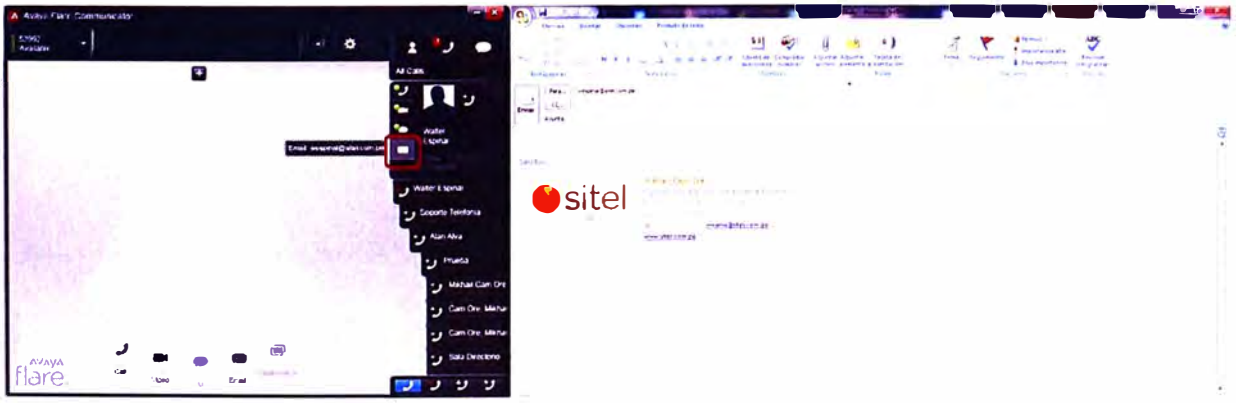


Figura 4.151 Envío de correos desde Avaya Flare Communicator para Windows

4.2.6. Verificación de Servicio de Avaya Video Collaboration Solutions

Tal como se vio anteriormente Avaya Video Collaboration Solutions incluye diversas alternativas para que los usuarios concreten sus conferencias de video, todas estas alternativas son compatibles y se integran entre sí tal como se describe en la figura.

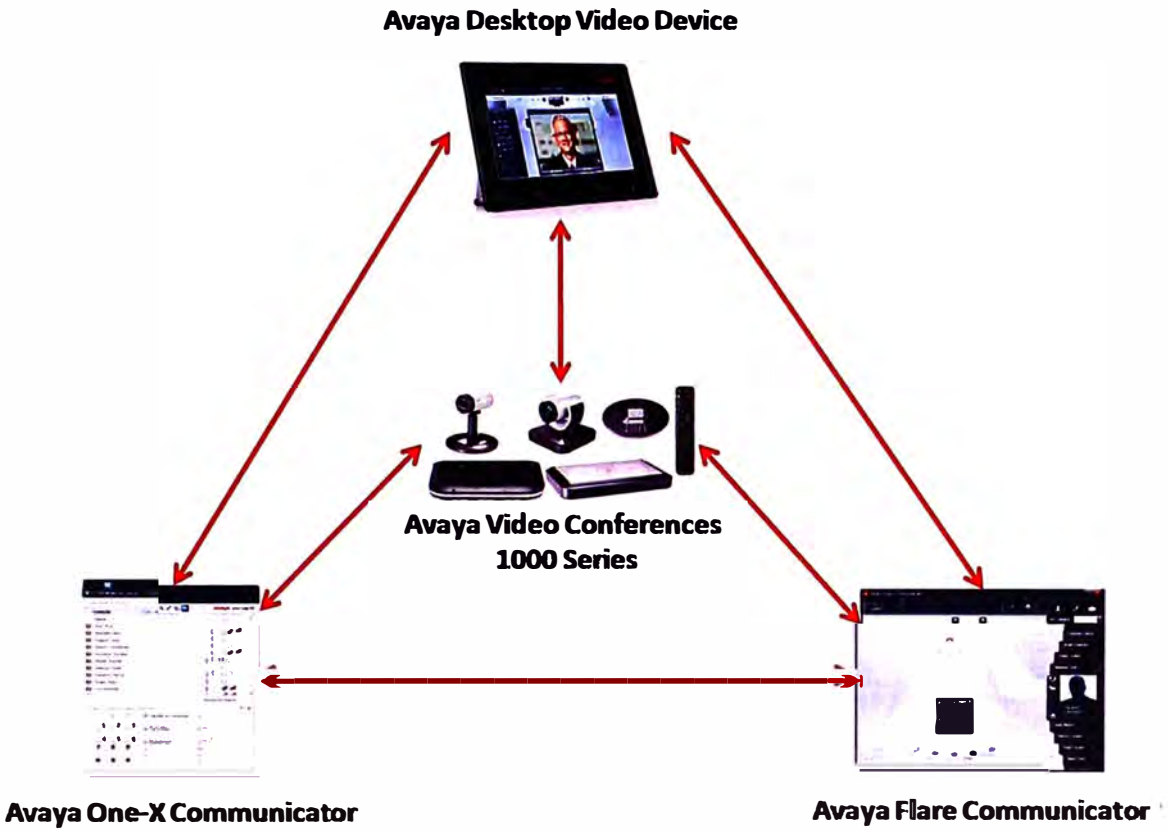
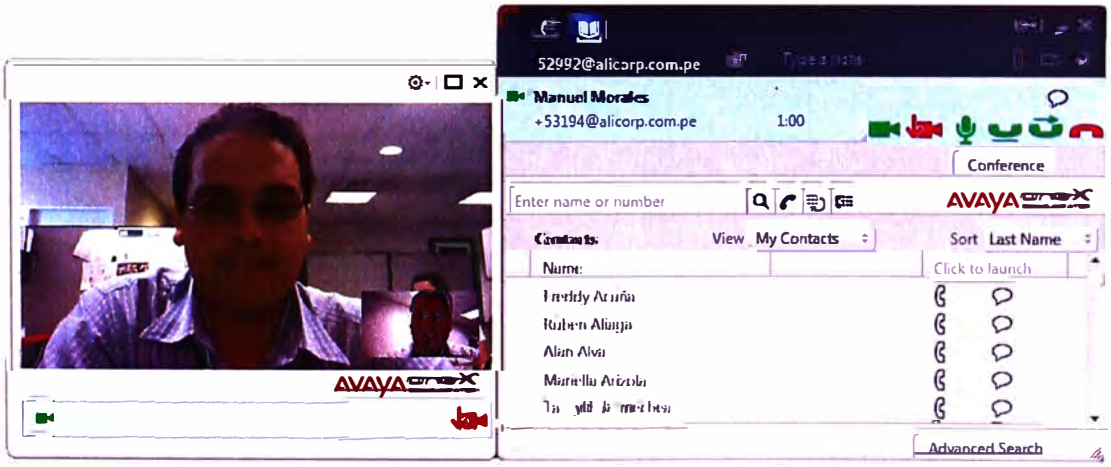


Figura 4.152 Integración de Avaya Video Collaboration Solutions

a. Avaya Desktop Video Device y Avaya One-X Communicator

Se verifica la conferencia de video punto a punto desde un usuario usando Avaya Desktop Video Device y otro usando Avaya One-X Communicator estableciéndose correcta calidad de video y audio



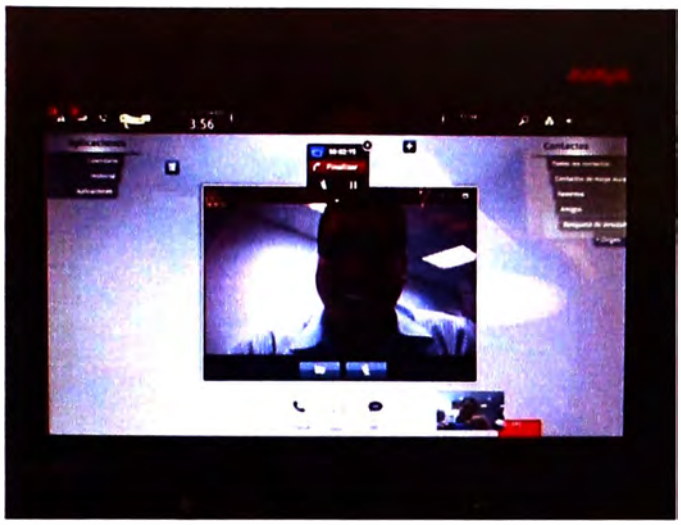


Figura 4.153 Videoconferencia entre Avaya Desktop Video Device y Avaya One-X Communicator

b. Avaya Desktop Video Device y Avaya Flare Communicator

Se verifica la conferencia de video punto a punto desde un usuario usando Avaya Desktop Video Device y otro usando Avaya Flare Communicator para Windows (la versión para iPad no incluye videoconferencias aún) estableciéndose correcta calidad de video y audio.

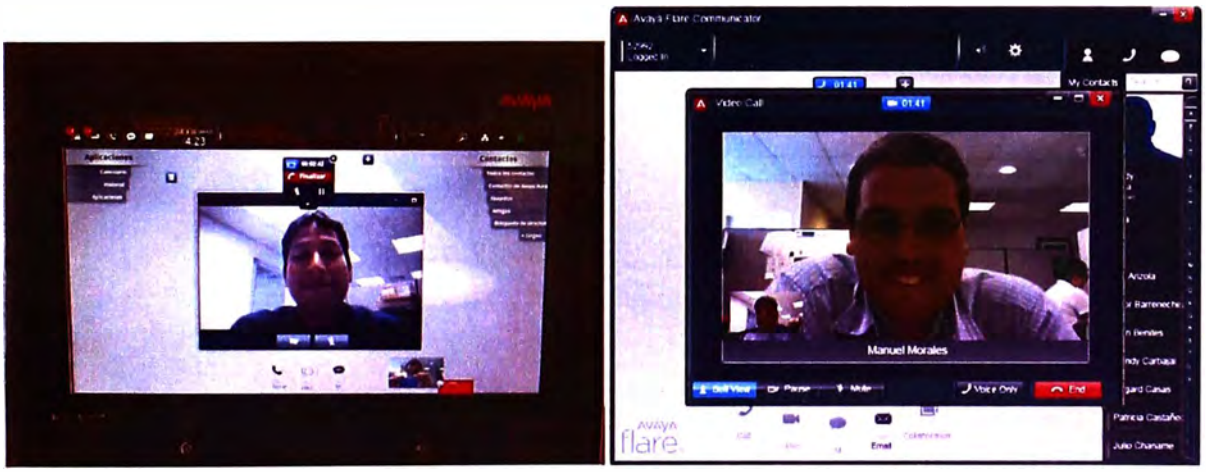


Figura 4.154 Videoconferencia entre Avaya Desktop Video Device y Avaya Flare Communicator

c. Avaya Desktop Video Device y Avaya Video Conference 1000 Series

Se verifica la conferencia de video punto a punto desde un usuario usando Avaya Desktop Video Device y otro usando una cámara Avaya Video Conference estableciéndose correcta calidad de video y audio.

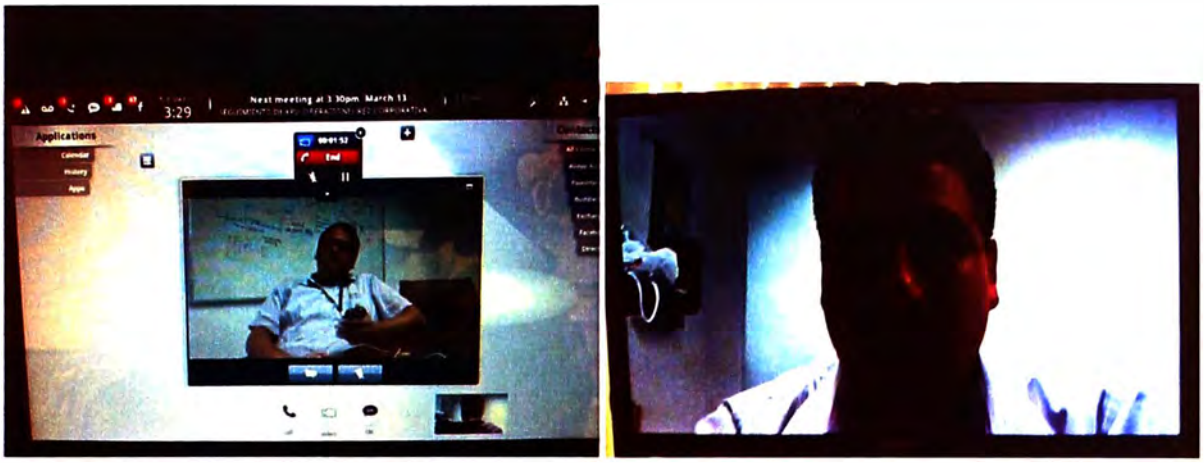


Figura 4.155 Videoconferencia entre Avaya Desktop Video Device y Avaya Video Conference

d. Avaya Video Conference 1000 Series y Avaya One-X Communicator

Se verifica la conferencia de video punto a punto desde un usuario con una cámara Avaya Video Conference y otro usuario utilizando Avaya One-X Communicator estableciéndose correcta calidad de video y audio.

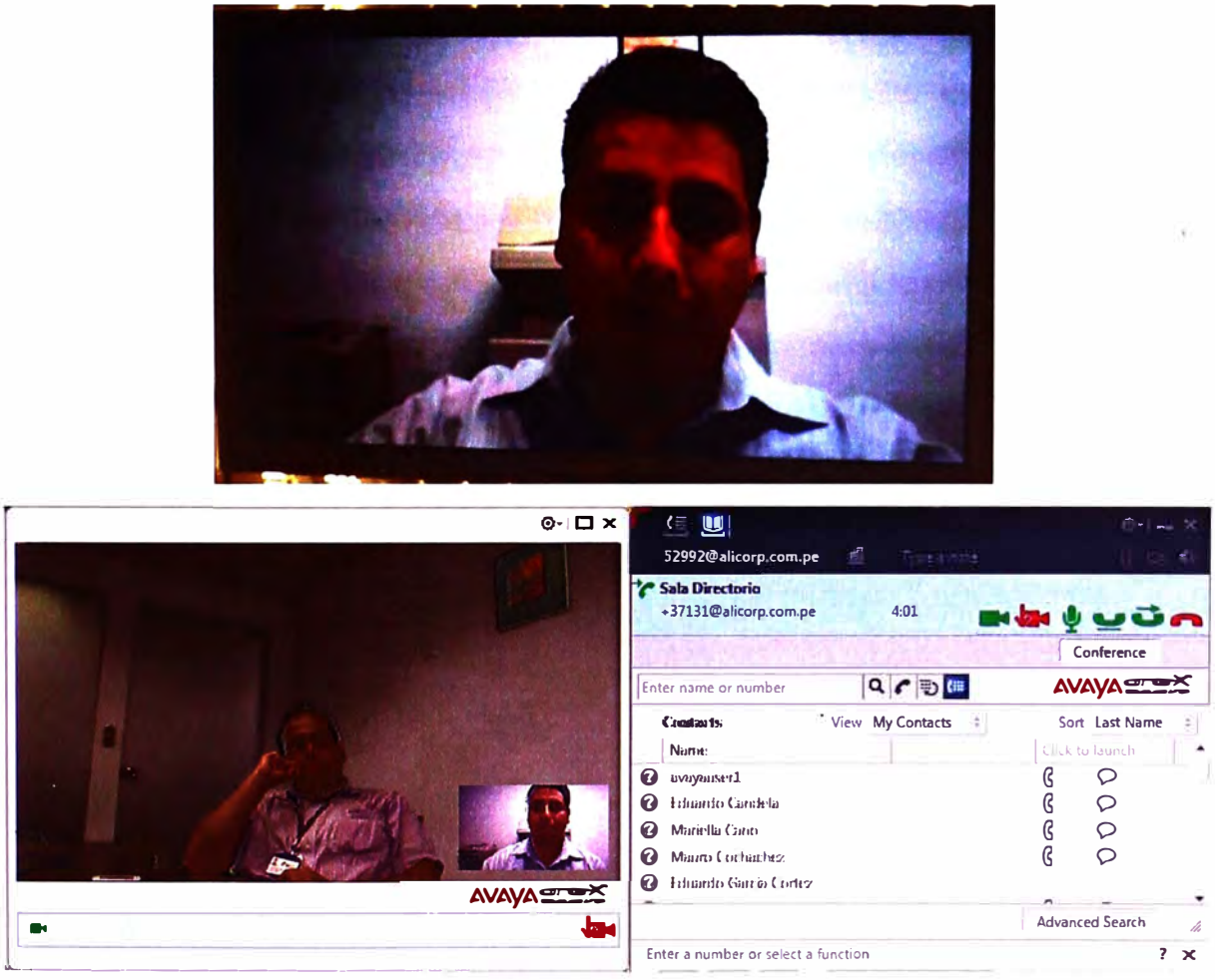


Figura 4.156 Videoconferencia entre Avaya Video Conference y Avaya One-X Communicator

e. Avaya One-X Communicator y Avaya Flare Communicator

Se verifica la conferencia de video punto a punto desde un usuario utilizando Avaya One-X Communicator y otro utilizando Avaya Flare Communicator estableciéndose correcta calidad de video y audio.

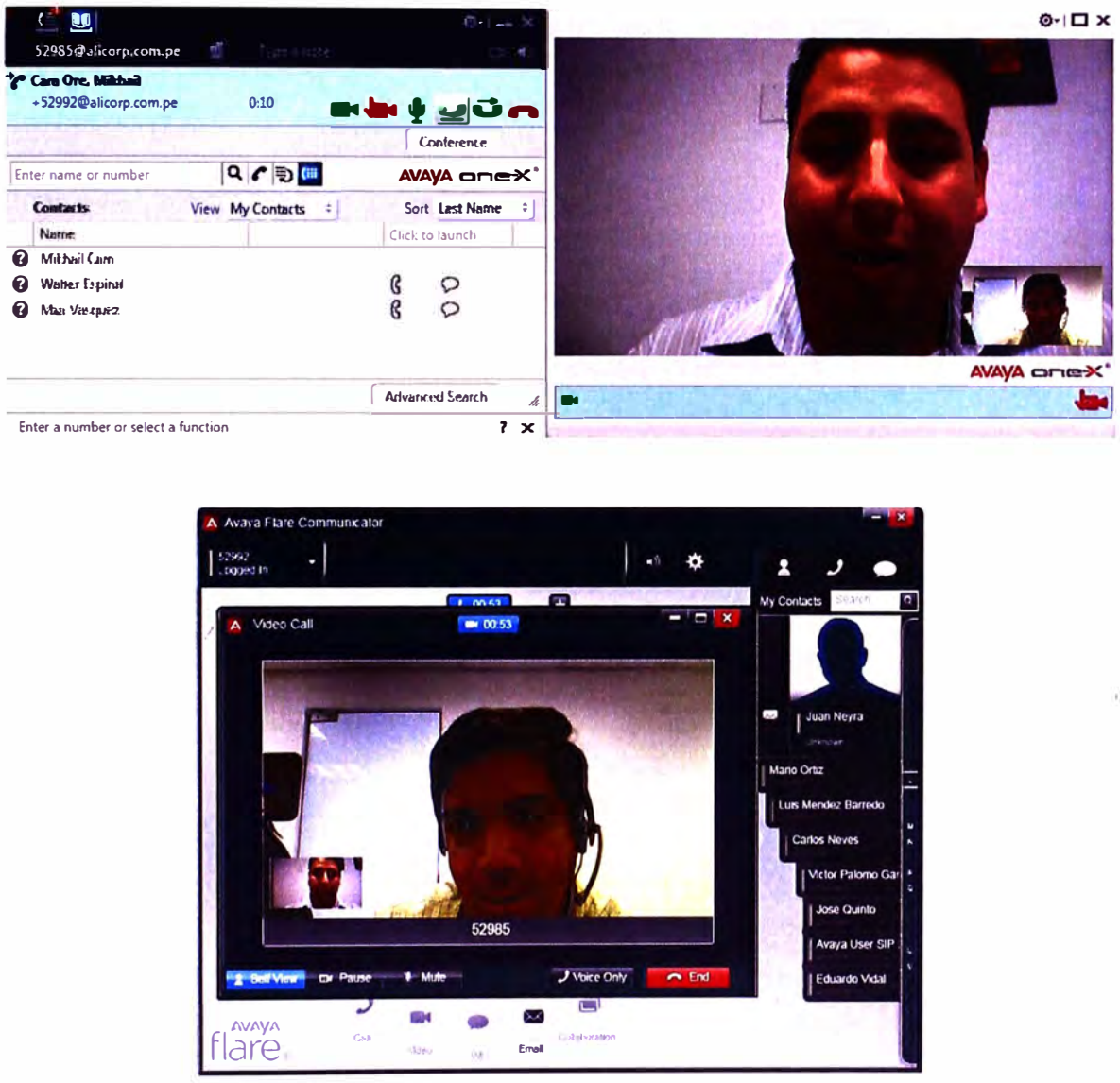


Figura 4.157 Videoconferencia entre Avaya One-X Communicator y Avaya Flare Communicator

f. Avaya Video Conference 1000 Series y Avaya Flare Communicator

Se verifica la conferencia de video punto a punto desde un usuario utilizando una cámara Avaya Video Conference y otro utilizando Avaya Flare Communicator estableciéndose correcta calidad de video y audio.

Figura 4.158 Videoconferencia entre Avaya Video Conference y Avaya Flare Communicator

4.2.7. Verificación de Servicio de Mensajería Instantánea

A continuación se verificará la facilidad de Mensajería Instantánea entre los dispositivos vistos en este informe que lo soportan, es decir Avaya Desktop Video Device, Avaya Flare Communicator y Avaya One-X Communicator.

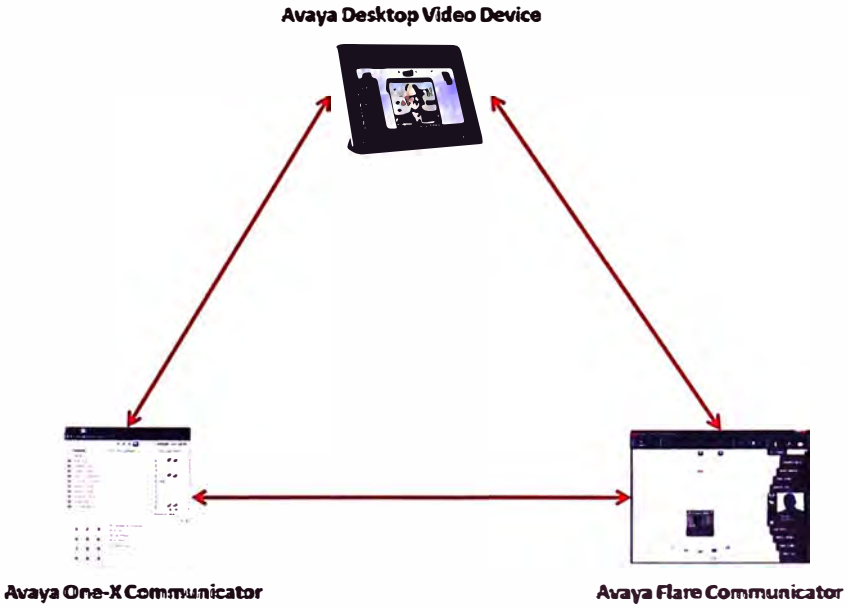


Figura 4.159 Integración para Mensajería Instantánea

a. Mensajería Instantánea entre Avaya Flare Communicator y Avaya One-X Communicator

Se verifica el correcto funcionamiento de la Mensajería Instantánea entre un usuario con Avaya Flare Communicator y otro con Avaya One-X Communicator. El usuario busca la ficha del contacto deseado y si tiene disponible el servicio de Mensajería Instantánea podrá abrir una ventana de chat para que puedan conversar.

Figura 4.160 Mensajería Instantánea en Avaya Flare Communicator

Se verifica el correcto intercambio de mensajes entre los usuarios, teniendo la posibilidad de pasar de una conversación de mensajería instantánea a una de voz utilizando sus botones respectivos.

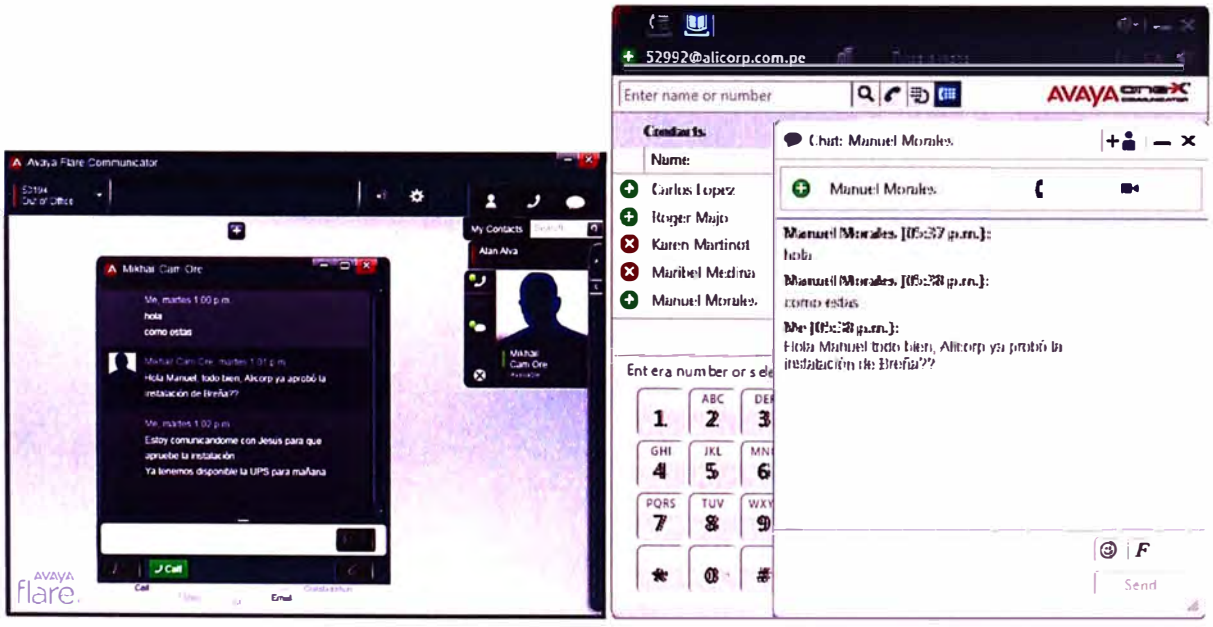


Figura 4.161 Mensajería Instantánea entre Avaya Flare Communicator y Avaya One-X Communicator

Se verifica el historial de Mensajería Instantánea en Avaya Flare Communicator, en donde se puede ver con quién se conversó, en qué día y a qué hora.

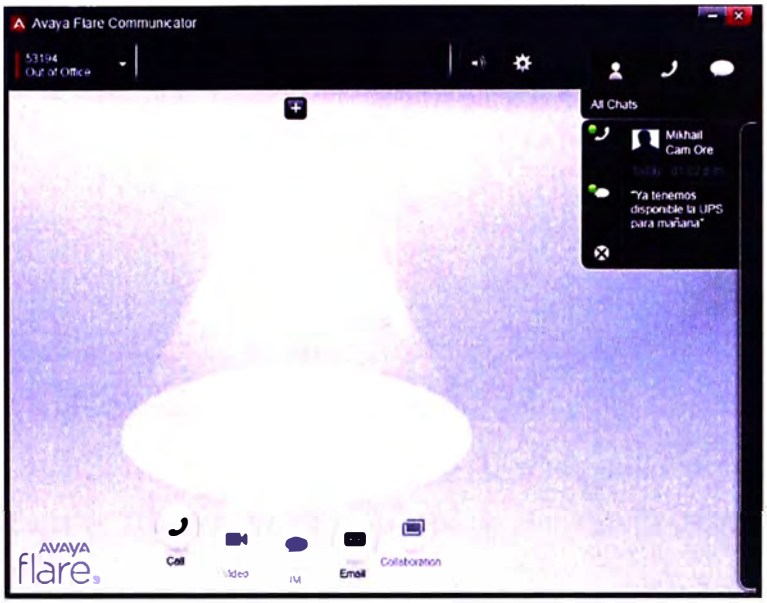


Figura 4.162 Registro de Mensajería Instantánea en Avaya Flare Communicator

Adicionalmente el Avaya One-X Communicator nos permite agregar a más usuarios dentro de la Mensajería Instantánea

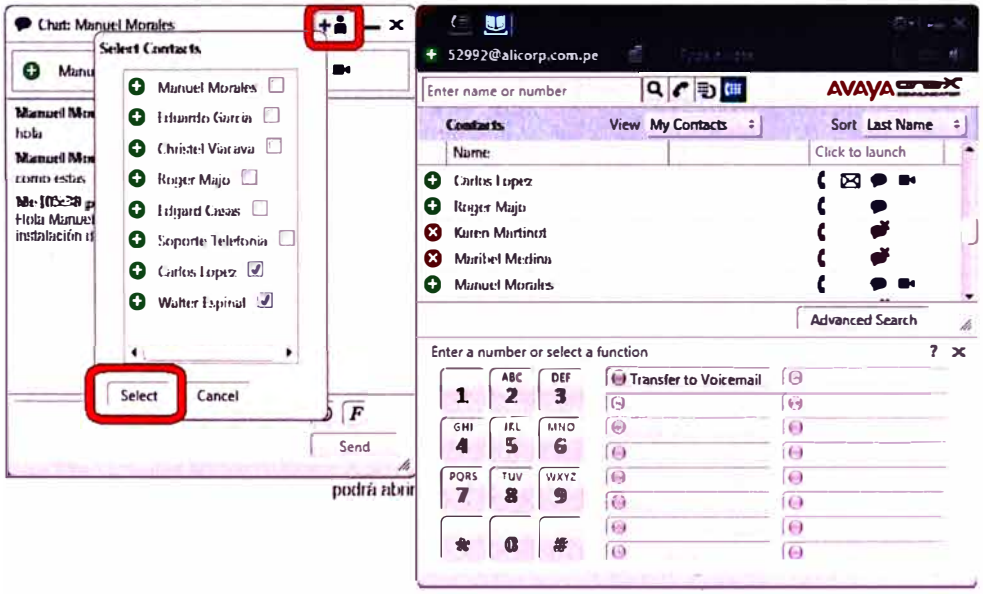


Figura 4.163 Registro de Mensajería Instantánea en Avaya Flare Communicator

b. Mensajería Instantánea entre Avaya Flare Communicator y Avaya Desktop Video Device

Se verifica el correcto funcionamiento de la Mensajería Instantánea entre un usuario con Avaya Flare Communicator y otro con Avaya Desktop Video Device. El usuario busca la ficha del contacto deseado y si tiene disponible el servicio de Mensajería Instantánea podrá abrir una ventana de chat para que puedan conversar.

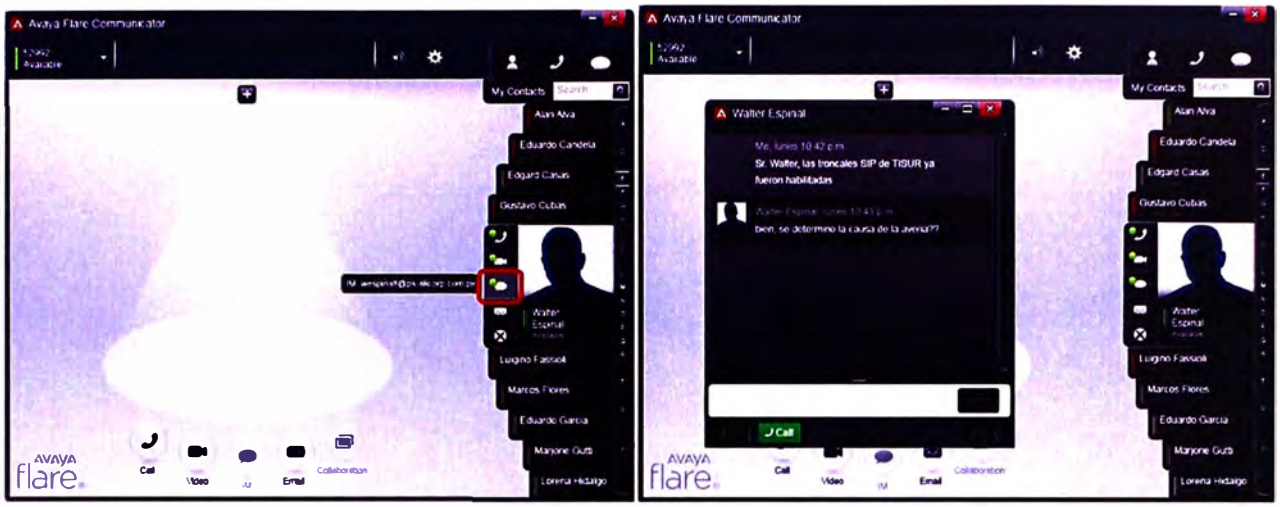


Figura 4.164 Mensajería Instantánea en Avaya Flare Communicator

Al usuario de Avaya Desktop Video Device le aparece un aviso en su pantalla para poder abrir la ventana de conversación y responder la Mensajería Instantánea.

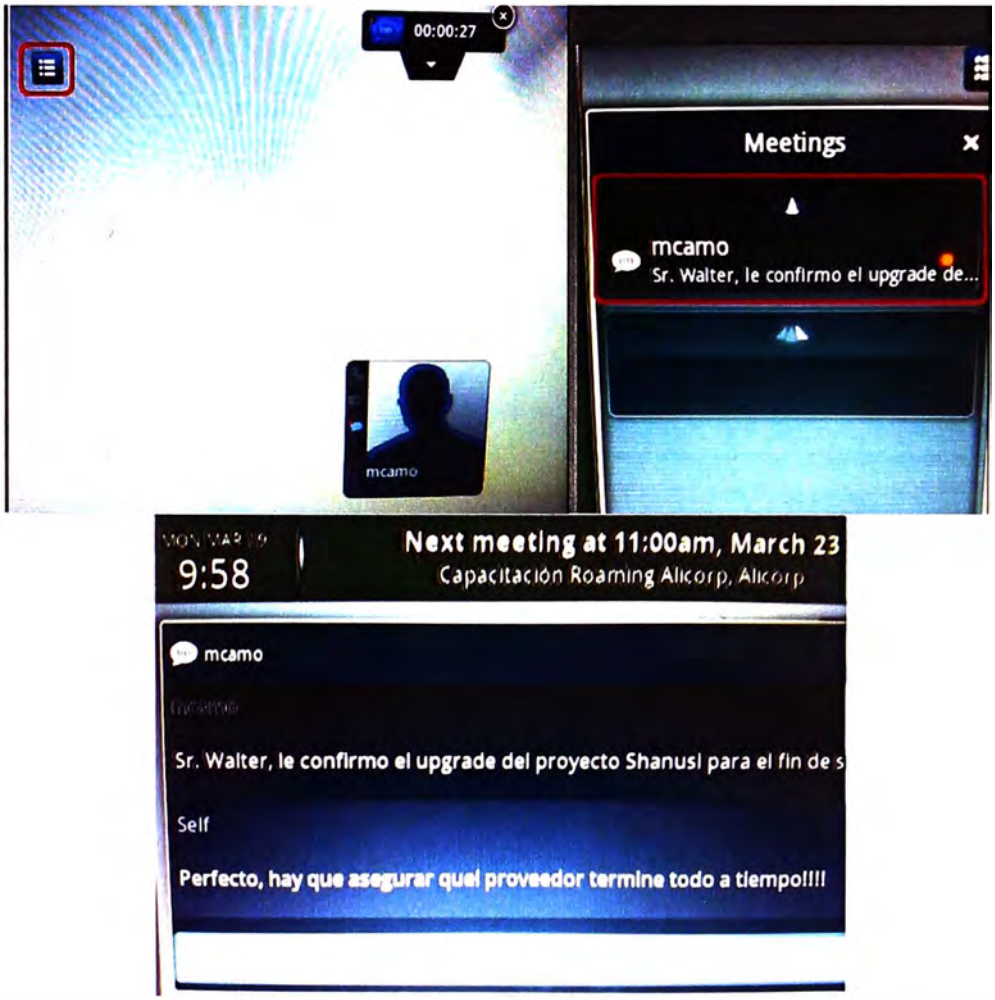


Figura 4.165 Mensajería Instantánea en Avaya Desktop Video Device

Se verifica el historial de Mensajería Instantánea en Avaya Desktop Video Device, en donde se puede ver con quién se conversó, en qué día y a qué hora.

Figura 4.166 Registro de Mensajería Instantánea en Avaya Desktop Video Device

c. Mensajería Instantánea entre One-X Communicator y Avaya Desktop Video Device

Se verifica el correcto funcionamiento de la Mensajería Instantánea entre un usuario con Avaya One-X Communicator y otro con Avaya Desktop Video Device. El usuario busca el contacto deseado y si tiene disponible el servicio de Mensajería Instantánea podrá abrir una ventana de chat para que puedan conversar.

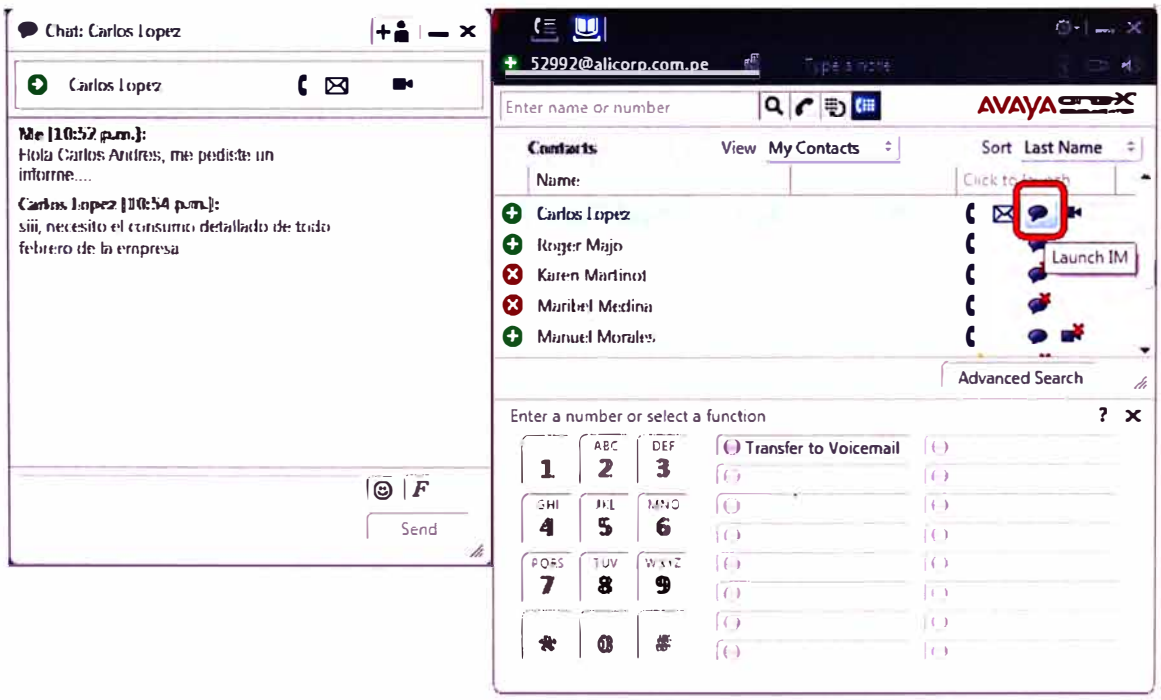


Figura 4.167 Mensajería Instantánea en Avaya One-X Communicator

Al usuario de Avaya Desktop Video Device le aparece un aviso en su pantalla para poder abrir la ventana de conversación y responder la Mensajería Instantánea.

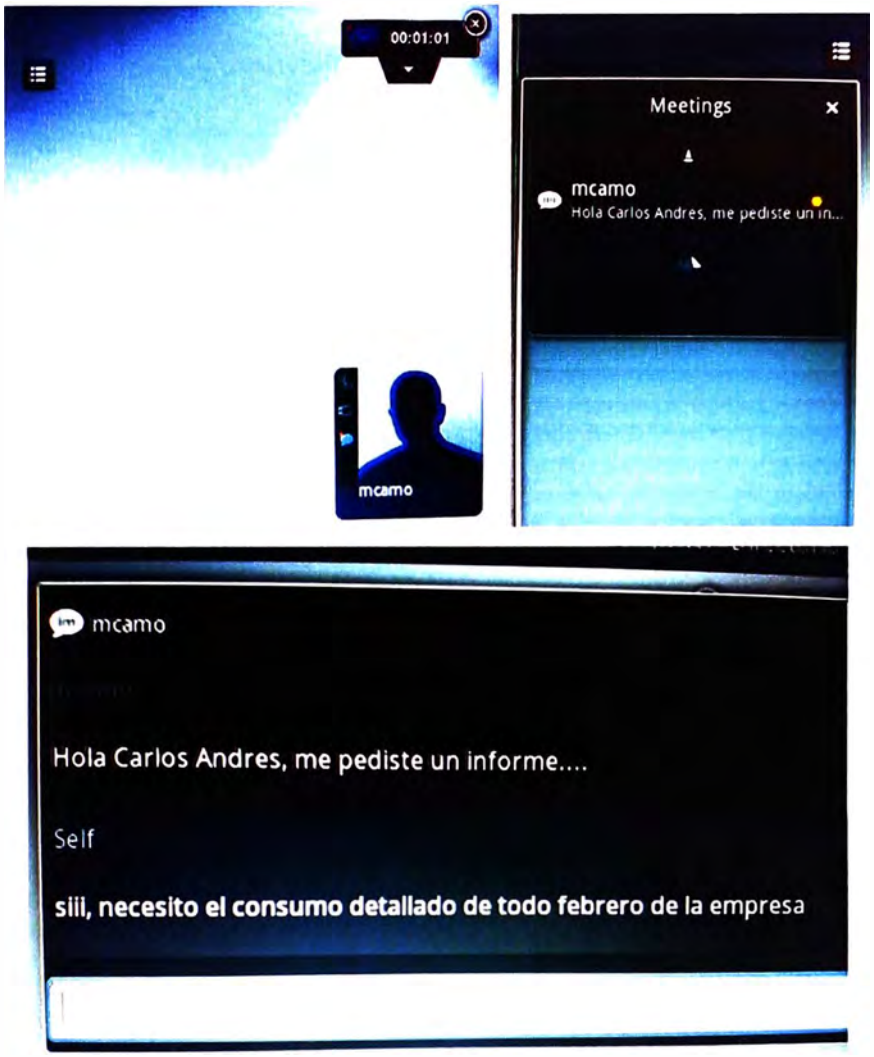


Figura 4.168 Mensajería Instantánea en Avaya Desktop Video Device

Se verifica el historial de Mensajería Instantánea en Avaya Desktop Video Device, en donde se puede ver con quién se conversó, en qué día y a qué hora.

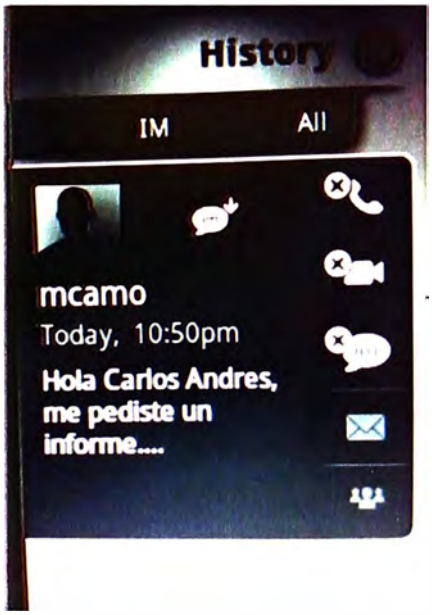


Figura 4.169 Registro de Mensajería Instantánea en Avaya Desktop Video Device

CAPITULO V
COSTOS DE LA SOLUCION

Lo detallado en los capítulos anteriores de este informe describe el funcionamiento de la Plataforma Aura 6.1 en la red corporativa de un grupo empresarial y las facilidades ofrecidas a los usuarios para cubrir sus necesidades de Comunicaciones Unificadas. Para detallar los costos de la implementación de esta plataforma debemos mencionar que se realizó en 2 etapas.

La primera consistió en la implementación del Aura Core 5.2 (Avaya Communication Manager, Avaya Session Manager y Avaya System Manager), esto se realizó en el mes de Setiembre del 2010 y con un costo de USD 80000 (Sin I.G.V.), que según la cotización respectiva se incluía lo siguiente:

Tabla 5.1 Inventario de primera etapa de implementación

CÓDIGO	CANTIDAD	DETALLE
183441	1	CM S8500 MODEL
195313	1	COMPACT FLASH READER W/FLSHCRD RHS
216893	1	MGMT R6 SITEL ADMIN - STD/ENT ED LIC (ASA)
216896	1	MGMT R6 NTWK MGMT - ENT ED LIC
216899	1	SYSTEM MANAGER R6 LIC
225145	1	AVAYA AURATM R6 SFTW ENTTLEMENT LIC
225152	100	AURA ENT ED R6 1-100 NEW LIC
229410	100	SM R6.X USER LICENSE W/ENT ED
229411	50	SM R6.X USER LICENSE
405362641	4	PWR CORD USA
700451206	1	IA770/CMM R5.x MEDIA KIT
700464506	1	USB MODEM USR5637-OEM 56K ROHS 6
700465305	1	PW9130 1500 120V RACK W /SNMP CARD
700477094	1	CM MESSAGING R6 MEDIA KIT
700478589	1	S8800 SRVR SMGR
700479439	1	PROGNOSIS VOIP MONITORING CD R2
181417	65	SIP TRUNK 1PT SFTW LIC
182746	50	EC500 OUTBOARD PROXY SIP LIC: NU
227571	50	AES 5.X BSC TSAPI RTU
228744	100	UCE R5.2 + ONE-X MBL R1/5.X CLIENT /E

228745	100	UCE R5.2 + ONE-X COMM R5.X SFTW /E
228746	100	UCE R5.2 + ONE-X PORTAL R5.X STD /E
228747	100	UCE R5.2 + AE SVCS R5.X UNFD DSKTP /E
228932	100	UCE R5.2 + EC500 R8.X SM LIC /E
228933	100	UCE R5.2 + IP SOFTPHONE R6.X LIC /E
228993	1	S8800 SERVER SESSION MGR
229762	100	UCE R5.2.1 STD/W CMEE 5.2 NEW SEAT 1
405362641	3	PWR CORD USA
700381254	1	COMPACT FLASH 128MB RHS
700406101	1	DS1 LOOPBACK JACK 700A RHS
700407802	1	G450 MP80 W/POWER SUPPLY
700466626	1	MM711 ANLG MEDIA MODULE - NON GSA
700466634	1	MM710B E1/T1 MEDIA MODULE - NON GSA
700470065	1	AVAYA AURATM R6.0 NEW SFTW CD
700470073	1	AVAYA AURATM R6.0 UPG SFTW CD
700500189	1	AES 5.2.1 SFTW ONLY MEDIA
174066	1	SOFTCON REGISTRATION MIGRATION
214372	1	OSPC CLIENT NEW USER LIC
214623	1	OSPC RFA ACTIVATION CODE NEW INSTALL
227945	5	ONE-X VIDEO R5.2.1 NEW ONE LIC
405362641	4	PWR CORD USA
700395445	1	120A CSU CABLE 50FT RHS
700405673	3	IP PHONE 9630G GRY 9630GD01A
700419195	3	IP PHONE 9640G GRY
700434897	4	1151D1 IP PHONE PWR W/CAT5 CBL
700451156	1	OSPC CLIENT USER SFTW CD
700461205	3	IP PHONE 9620C CHARCOAL GRY
700461213	3	IP PHONE 9650C CHARCOAL GRY
228990	1	S8800 SERVER CM 5.2.1
232320	1	S8800 MIGRATION KIT
195476	1	SOFTWARE SUPPORT COMMUNICATION MGR MODEL
219056	50	SSU AES R5.X BSC TSAPI AN
219286	5	SSU ONE-XC R1/R5 VIDEO ACT AN
219651	100	SSU AURA R6.X ENT ED 1-100 AN
219892	100	SSU UCE R5.2+ ONE-X MBL R1/5.X CLNT /E
219893	100	SSU UCE R5.2+ ONE-X COMM R5.X SFTW /E
219894	100	SSU UCE R5.2+ ONE-X PORTAL R5.X STD /E
219895	100	SSU UCE R5.2+ AES R5.2+ UNFD DSKTP /E
219896	100	SSU UCE R5.2+ EC500 R8.X SINGLE MODE /E
219897	100	SSU UCE R5.2+ IP SOFTPHONE R6.X /E
219905	50	SSU SM R6.X USER AN

La segunda etapa consistió en la implementación de los servidores de aplicaciones como son Avaya One-X Portal, Avaya One-X Mobile y Avaya Presence Services, esto se realizó en los meses de Enero y Marzo del 2011 con un costo de USD 16510 (Sin I.G.V.) que se detalla a continuación:

Tabla 5.2 Inventario de segunda etapa de impementación

CODIGO	CANTIDAD	DETALLE
Servidor One-X Portal		
7944G2U	1	x3550 M3, Xeon 4C E5640 80W 2.66 Ghz/1066Mhz/12MB, 1x4GB, O/Bay 2.5in HS SAS/SATA, SR M5014, 675W p/s, Rack
59Y4008	1	Intel Xeon 4C Processor Model E5640 80W 2.66 Ghz/1066Mhz/12MB
49Y1435	3	4GB (1x4GB, 2Rx4, 1.5V) PC3-10600 CL9 ECC DDR3 1333MHz LP RDIMM
42D0677	3	IBM 146 GB 2.5in SFF Slim-HS 15K 6Gbps SAS HDD 3
59Y3952	1	IBM System x3550 M3 R2 ODD Kit
46M1075	1	IBM 675W Redundant AC Power Supply
44R9271	1	Red Hat Enterprise Linux for x86 Standard Subscription 1 Yr Subscription
46M0901	1	IBM UltraSlim Enhanced SATA DVD-ROM
Servidor One-X Mobile		
7944B2U	1	x3550 M3, Xeon 4C E5507 80W 2.26GHz/800MHz/4MB, 1x4GB, O/Bay 2.5in HS SAS/SATA, SR M1015, 675W p/s, Rack
42D0677	2	IBM 146 GB 2.5in SFF Slim-HS 15K 6Gbps SAS HDD
59Y3952	1	IBM System x3550 M3 R2 ODD Kit
46M1075	1	IBM 675W Redundant AC Power Supply
44R9271	1	Red Hat Enterprise Linux for x86 Standard Subscription 1 Yr Subscription
46M0901	1	IBM UltraSlim Enhanced SATA DVD-ROM
Presence Services		
7945B2U	1	x3650 M3, Xeon 4C E5507 80W 2.26GHz/800MHz/4MB, 1x4GB, O/Bay 2.5in HS SAS/SATA, SR M1015, 675W p/s, Rack
59Y4016	1	Intel Xeon 4C Processor Model E5507 80W 2.26GHz/800MHz/4MB
49Y1435	7	4GB (1x4GB, 2Rx4, 1.5V) PC3-10600 CL9 ECC DDR3 1333MHz LP RDIMM
42D0677	5	IBM 146 GB 2.5in SFF Slim-HS 15K 6Gbps SAS HDD
46M0832	1	ServeRAID M1000 Series Advance Feature Key
46M1075	1	IBM 675W Redundant AC Power Supply
44R9271	1	Red Hat Enterprise Linux for x86 Standard Subscription 1 Yr Subscription
46M0901	1	IBM UltraSlim Enhanced SATA DVD-ROM

Todos estos costos mencionados han tenido un descuento de alrededor del 50% en ambas etapas, esto gracias a que el Grupo empresarial sobre el cual se ha trabajado en el presente informe cuenta con un Contrato Beta con el fabricante Avaya. El Contrato Beta es una asociación que el fabricante Avaya hace con clientes estratégicos para evaluar el rendimiento de sus productos nuevos en escenarios de uso real recogiendo las observaciones que estos clientes hagan sobre dichos productos.

Fue así que las versiones de software de los servidores en cuestión han ido actualizándose a medida que la Plataforma Aura ha ido implementándose como por ejemplo:

- Los costos mencionados en los cuadros de este capítulo son por la implementación de Aura Core 5.2 según cotización entregada por el proveedor en Mayo 2010. En la fecha de implementación (Setiembre 2010) ya existía Aura Core 6.0 y esa fue la que se instaló. Finalmente en Enero 2011 aparece Aura Core 6.1 y la plataforma es actualizada, siendo este reléase el centro de la investigación del presente Informe de Suficiencia. Estas actualizaciones no generaron costo alguno gracias al Contrato Beta que el Grupo tiene con el fabricante Avaya.

- Dado que Aura Core fue implementado en release 6.1, los servidores de aplicaciones cambiaron: El servidor de Avaya One-X Portal quedó sin ser utilizado, el servidor de Avaya One-X Mobile 5.2 se convirtió en Avaya One-X Client Enablement Services 6.1(Marzo del 2011) y el servidor Avaya Presence Services fue implementado en reléase 6.1 (Enero del 2011). Estas actualizaciones no generaron costo alguno Beta que el Grupo tiene con el fabricante Avaya.

- Los costos de la primera etapa de implementación consideran las licencias necesarias para la plataforma en su totalidad. Los costos mostrados en la segunda etapa consideran únicamente los servidores para aplicaciones dado que las licencias para estos ya fueron adquiridas en la primera etapa.

- La capacidad de la Plataforma Aura fue concebida para 100 usuarios de Comunicaciones Unificadas. Esta capacidad ha sido extendida a 200 usuarios sin costo alguno el mes de Febrero 2012 gracias al convenio Beta que el Grupo tiene con el fabricante Avaya.

- En los cuadros presentados en este capítulo se consideran 12 teléfonos IP comprados por el Grupo. Adicionalmente a estos Avaya entregó 10 equipos adicionales sin costo por participar en el Contrato Beta, posteriormente en Junio 2011 Avaya entrega 6 teléfonos IP sin costo por la participación de un Beta sobre firmware para teléfonos, y en Marzo 2012 Avaya entrega 15 teléfonos IP sin costo por la participación en otro Beta. Adicionalmente a todo muchos usuarios usaban también equipos Nortel 1220 que fueron registrados en Avaya Aura gracias a la conversión del firmware respectivo para que los equipos 1220 puedan comportarse como teléfonos SIP registrados en Avaya Session Manager, esto como medida de parte de Avaya para heredar el equipamiento ya existente y reutilizarlo.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Los usuarios tiene mayor libertad de movilidad, ya no necesitan estar ubicados necesariamente en sus sitios de trabajo pues Avaya Aura recibirá sus llamadas y les dará el tratamiento que ellos mismos decidan.
2. Los usuarios tiene flexibilidad para modificar el tratamiento de las llamadas y disponen de varias alternativas para mantenerse comunicados con sus empresas desde el lugar que deseen y utilizando el dispositivo que gusten.
3. Los usuarios pueden manejar un solo número de contacto que sería el número público directo de su anexo (DID), pues Avaya Aura recibirá las llamadas en el anexo del usuario y le dará el tratamiento que este haya requerido.
4. Los procesos de las empresas mejoran a razón de que los usuarios tienen mayor disponibilidad y los tiempos de respuesta se reducen, las consultas son absueltas en menor tiempo.
5. Para las empresas que tienen colaboradores que viajan constantemente las soluciones de comunicaciones unificadas las ayuda a ahorrar grandes montos por concepto de roaming. Un usuario que viaje al extranjero ya no necesita llevar su móvil con servicio de roaming activo para recibir sus llamadas pues con la plataforma Avaya Aura puede derivar las llamadas entrantes hacia un número local del país visitado que el mismo usuario defina; de igual manera si el usuario desea llamar a algún número telefónico de Perú puede hacer llamadas con costo local usando las troncales de Avaya Aura de forma remota.
6. Manejar las Comunicaciones Unificadas de manera centralizada hace más sencilla su administración y monitoreo. Por lo tanto, la resolución de incidencias es también más simple.
7. Se invierte en una sola plataforma y los servicios están disponibles para todas las empresas del Grupo Empresarial.

Recomendaciones

1. Se recomienda aplicar redundancia geográfica habilitando un Aura Core (Avaya Session Manager, Avaya Communication Manager y Avaya System Manager) en otro sitio dentro de la red del Grupo.
2. Se recomienda darle mantenimiento general a los servidores que conforman la plataforma Avaya Aura por lo menos una vez al año.
3. Se recomienda que las instalaciones donde estén instalados los servidores deben contar con la refrigeración adecuada para evitar cualquier daño por calentamiento interno. Asimismo deben contar con una puesta a tierra con una impendancia no mayor de 5 ohmios como protección eléctrica.
4. Se recomienda revisar periódicamente la web del fabricante para descargar las actualizaciones de software más reciente y aplicarlas a la Plataforma Avaya Aura.
5. Se recomienda capacitar en forma detallada a los usuarios que harán uso de los servicios de Comunicaciones Unificadas para su correcto uso y sean bien aprovechados.
6. Configurar las cuentas VPN de los usuarios de tal forma que aseguren un ancho de banda considerable para asegurar una buena calidad de voz en el caso del uso de aplicativos fuera de la red corporativa.

ANEXOS

ANEXO A
INSTALACION DE SYSTEM PLATFORM

Lo primero que hacemos para instalar el System Platform en el servidor deseado es insertarle el CD de Instalación y reiniciarlo para que lo ejecute. Nos aparecerá una imagen similar a la mostrada y presionamos Enter para que inicie la instalación.

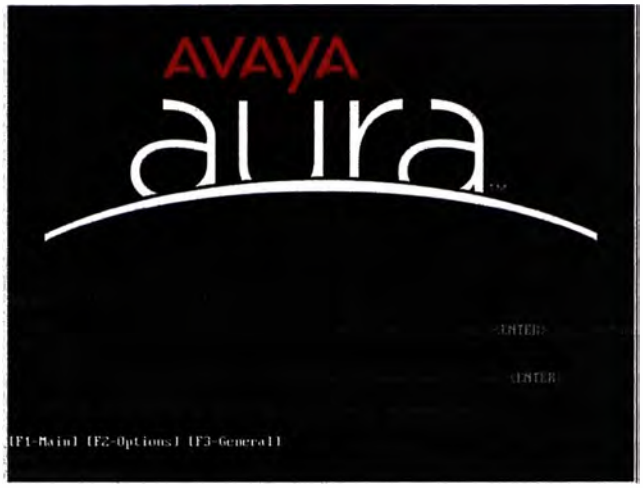


Figura A.1 Inicio de instalación de System Platform

Lo primero que nos consultan es el tipo de teclado que estamos usando.

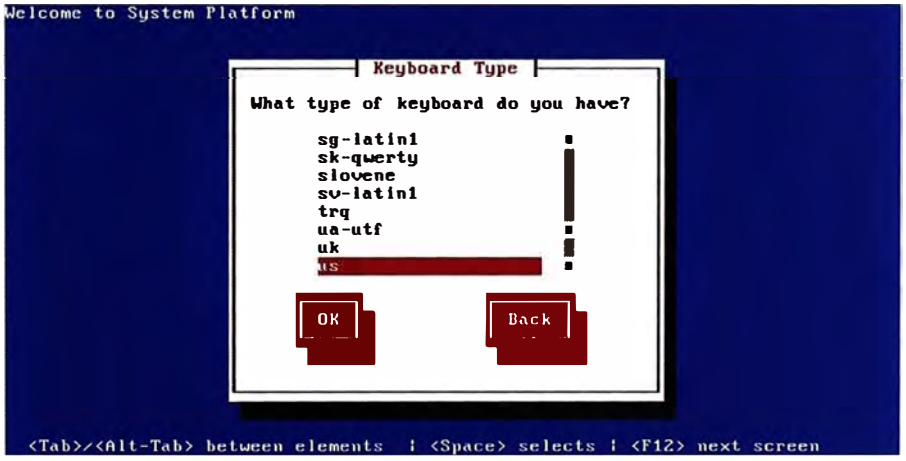


Figura A.2 Tipo de teclado

Colocamos la información de configuración de red necesaria como la dirección IP de System Patform, máscara de red, default Gateway y dirección IP del DNS.

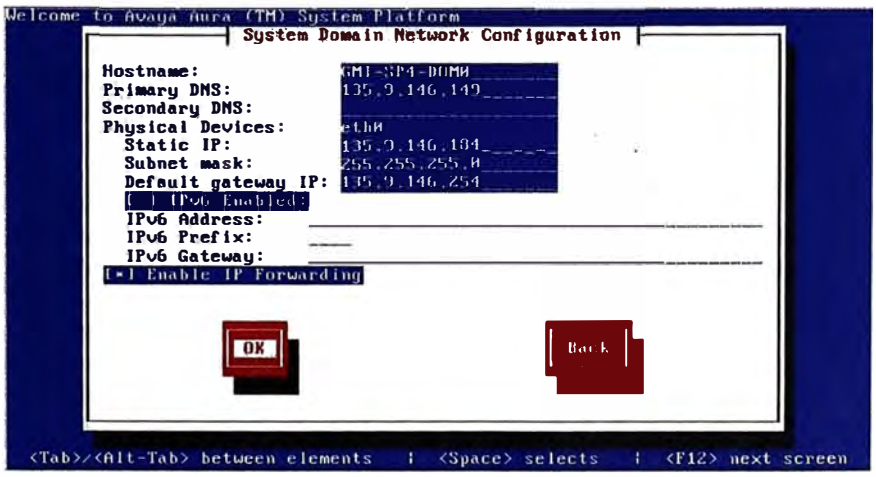


Figura A.3 Configuración de red para System Platform

Luego confirmamos la facilidad de *IP forwarding*, que nos permitirá acceder por consola web al servidor y a las máquinas virtuales que se vayan a instalar luego sobre System Platform.

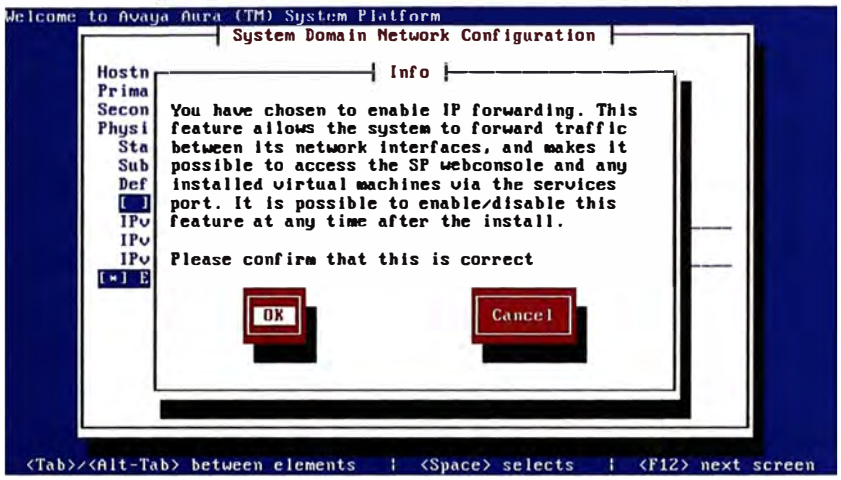


Figura A.4 IP forwarding para System Platform

Luego ingresamos los datos del Console Domain (CDOM)

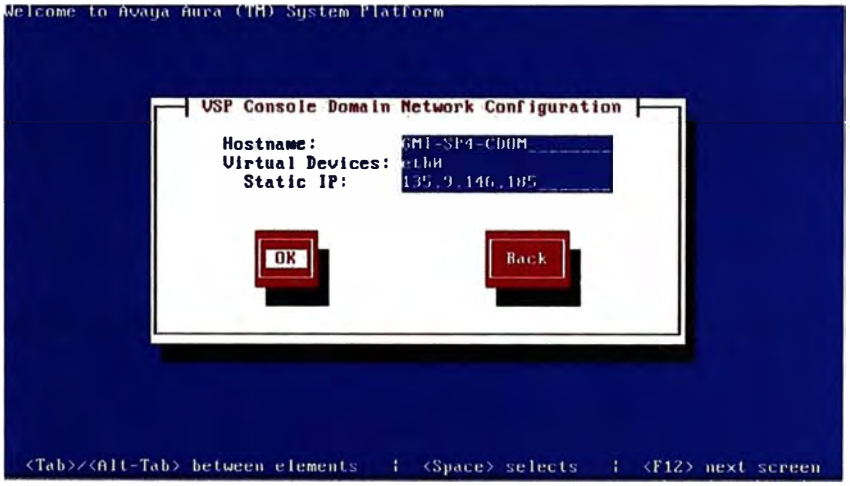


Figura A.5 Datos para Console Domain

Confirmamos luego la Zona Horaria que nos corresponde.

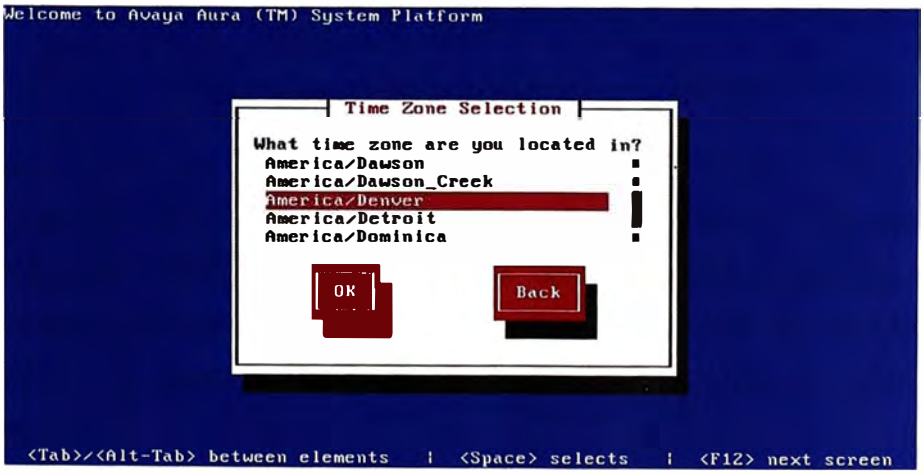


Figura A.6 Datos de Zona Horaria

Asignamos las contraseñas respectivas para las cuentas root, admin, cust y LDAP del servidor.

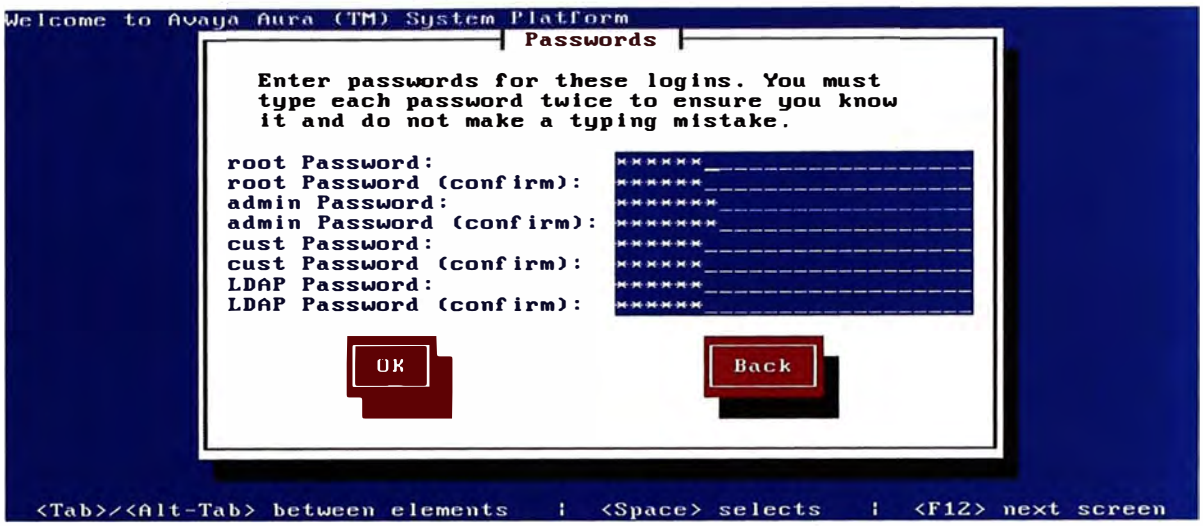


Figura A.7 Contraseñas para System Platform

Con esto se inicia el proceso de instalación de System Platform

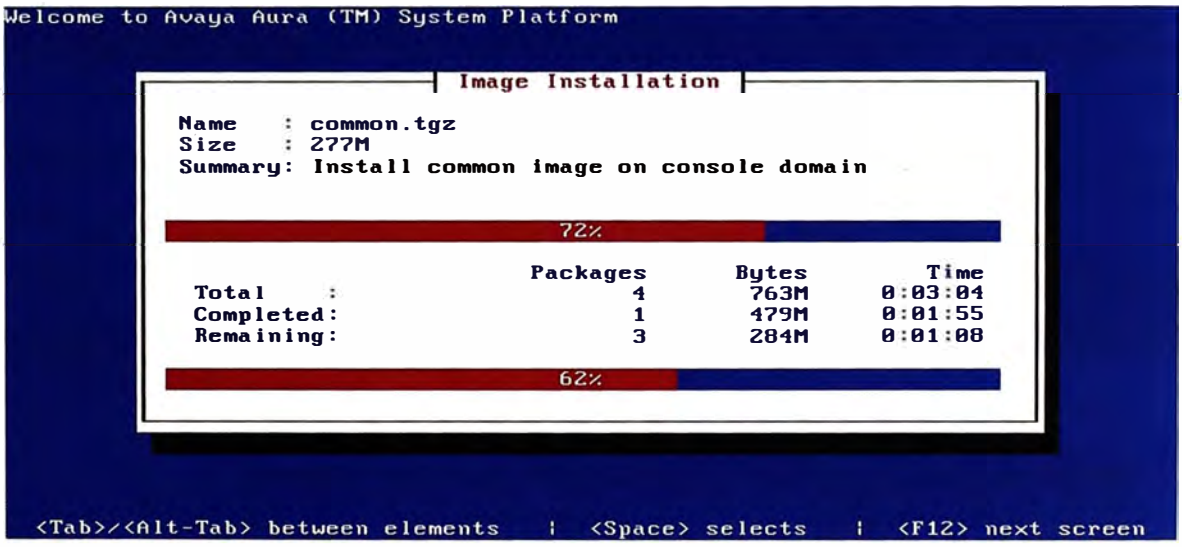


Figura A.7 Instalación de System Platform

Cuando ese proceso haya concluido ingresamos a la consola de comandos del servidor y nos logueamos con la cuenta admin, luego revisamos las entradas declaradas en el archivo hosts (*cat /etc/hosts*). Encontraremos correctamente declarados al cdom y domain-0. Podemos entonces ejecutar el comando ssh dom0.vsp, si la consola acepta el password que le ingresamos tenemos la seguridad de que el System Platform ha iniciado correctamente.

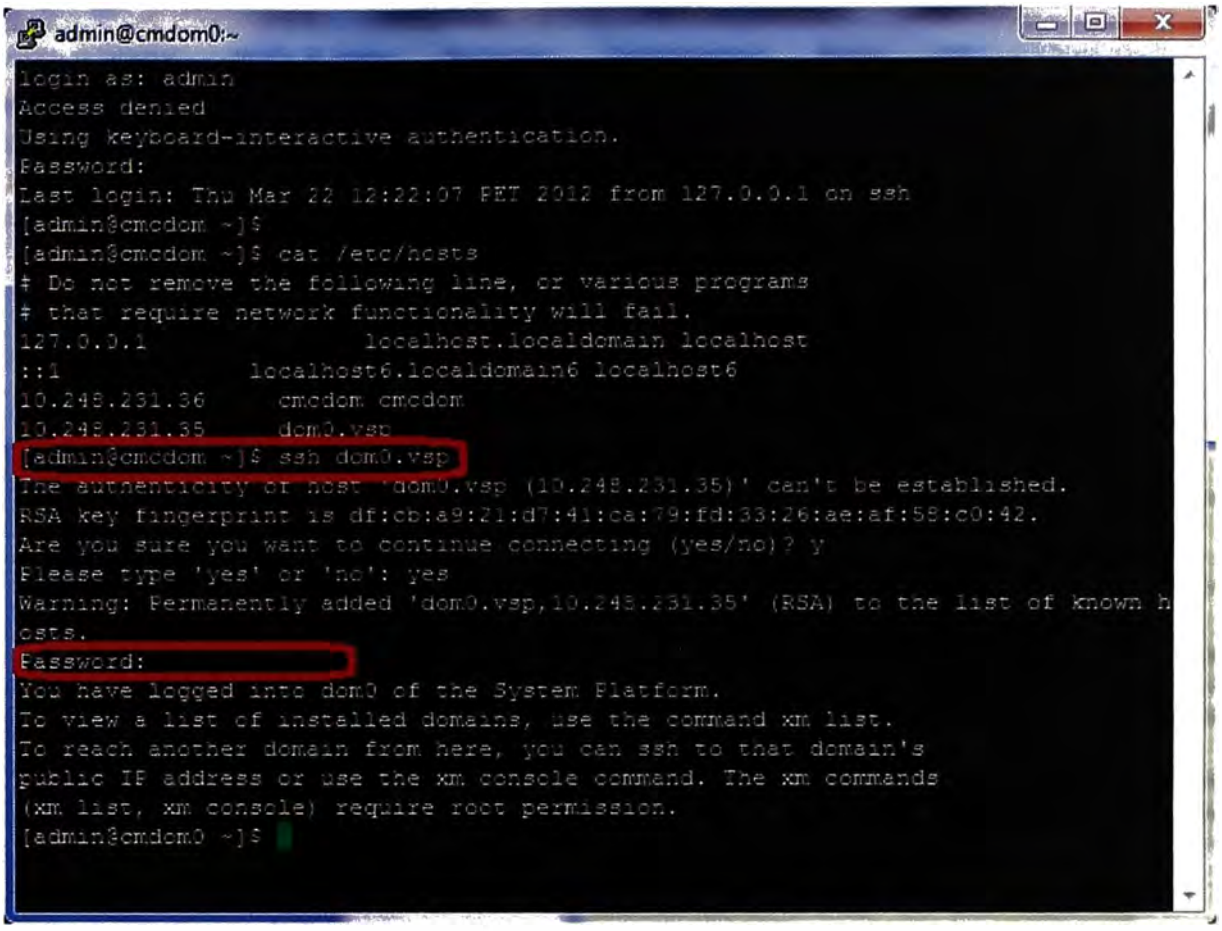


Figura A.8 Consola de Comandos para System Platform

Para confirmar ingresamos vía web a *http://ipaddress/* y nos autenticamos con la cuenta *admin*.

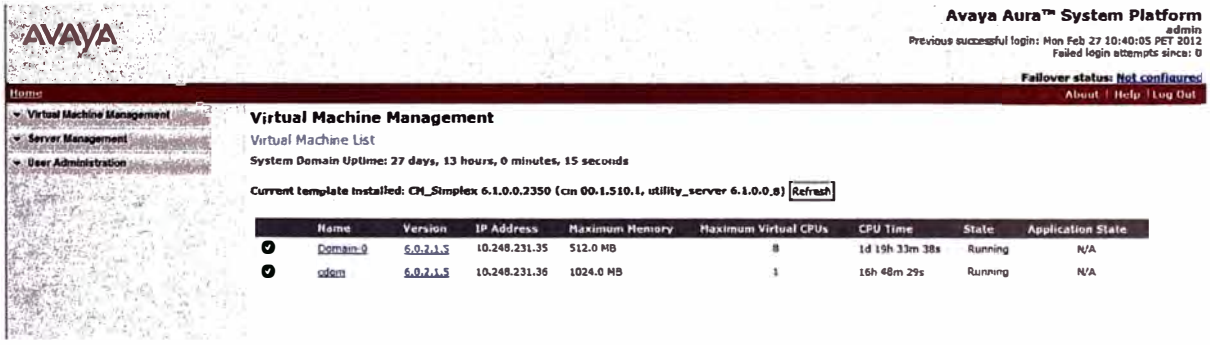


Figura A.9 Verificación de System Platform

ANEXO B
GLOSARIO DE TERMINOS

ATM Asynchronous Transfer Mode
ADVD Avaya Desktop Video Device
CSCF Call State Control Function
CIC Circuit Identification Code
COR Class of Restriction
COS Class of Services
CES Client Enablement Services
CM Communication Manager
CPE Customer Provided Equipment
DES Data Encryption Standard
DLCI Data Link Connection Identifier
DVD Digital Versatile Disc
DNS Domain Name System
DHCP Dynamic Host Configuration Protocol
FEC Forwarding Equivalence Class
GPRS General Packet Radio Service
HSS Home Suscriber Server
HTTPS Hypertext Transfer Protocol Secure
HTTP Hypertext Transport Protocol
IM Instant Messaging
INAP Intelligent Network Application
IMAP Internet Message Access Protocol
IP Internet Protocol
IPSec Internet Protocol Security
IMS IP Multimedia System
ISUP ISDN User Part
LSP Label Switch Path
LSR Label Switching Router
LIFO Last In, First Out
LDAP Lightweight Directory Access Protocol
LAN Local Area Network
MCU Multipoint Control Unit
MPLS Multiprotocol Label Switching
PoE Power over Ethernet
PS Presence Services
PBX Private Branch Exchange

PSTN	public switched telephone network
RTP	Real-Time Transport Protocol
RTC	Red Telefónica Conmutada
RFC	Request For Comments
RIM	Research In Motion
RSA	Rivest, Shamir y Adleman
SLA	Service Level Agreement
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SM	Session Manager
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SMGR	System Manager
TDM	Time-division multiplexing
3DES	Triple DES (Data Encryption Standard)
UC	Unified Communication
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UMTS	Universal Mobile Telecommunications System
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
VCI	Virtual Channel Identifier
VLAN	Virtual Local Area Network
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network

BIBLIOGRAFIA

[1] Accelerating Unified Communications With an Enterprise-Wide Architecture
http://www.e-telsystems.com/documents/Accelerating_Unified_Communications.pdf

[2] SIP: Session Initiation Protocol
http://www.efort.com/media_pdf/SIP_ESP.pdf

[3] Redes Privadas Virtuales
http://www.ilustrados.com/documentos/redes-privadas-virtuales-110308.pdf

[4] IP Multimedia
www.uv.es/~montanan/redes/trabajos/IP_Multimedia.doc

[5] Comunicaciones Unificadas para dummies
https://www.avaya.com/es/registration/comunicaciones-unificadas-para-dummies/

[6] Avaya Aura
http://www1.cala.avaya.com/Mexico/Campaigns/Q309/Beat_Competition_T3/PDFs/Avaya_Aura.pdf

[7] Installing and Configuring Avaya Aura System Platform
https://support.avaya.com/css/P8/documents/100068113

[8] Installing and Configuring Avaya Aura System Manager
http://support.avaya.com/css/P8/documents/100072072

[9] Installing and Configuring Avaya Aura Communication Manager
http://support.avaya.com/css/P8/documents/100089133

[10] Administering Avaya Aura Communication Manager
http://support.avaya.com/css/P8/documents/100089333

[11] Installing and Configuring Avaya Aura Session Manager
http://support.avaya.com/css/P8/documents/100089152

[12] Implementing Avaya Aura Presence Services 6.1 Service Pack2
http://support.avaya.com/css/P8/documents/100133523

[13] Implementing Avaya Aura One-X Client Enablement Services
http://support.avaya.com/css/P8/documents/100148643